



Internet and Smartphone Privacy Explained and Made Easy

by
Dan Rosenthal and Tom Lundin

Internet and Smartphone Privacy Explained and Made Easy

Dan Rosenthal
Tom Lundin

Originally published by
Renegade Gold Advisory, Inc.

First edition

© 2017 by Dan Rosenthal & Tom Lundin
All rights reserved

Revised edition

© 2018 by Tom Lundin
All rights reserved

No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, without the prior permission of the copyright owners and the above publisher of the book.

IMPORTANT NOTE:

The phone numbers and e-mail addresses for Renegade Gold Advisory, Inc. contained within the text are no longer in service.

Foreword

Internet and Smartphone Privacy Explained and Made Easy

Most people never think twice about their email getting hacked. Hillary was one of them, and it cost her the Presidency.

Ignoring the danger probably won't cost you the Presidency but it opens the door to costly, time consuming catastrophic problems, including for instance having your identity stolen.

You wake up one morning sort through the mail and find a bill for something you didn't buy. Then another, and another.

You're wondering what the heck is going on, and call your bank only to find your bank account was emptied.

You go to the ATM to pick up some cash for the day, and you find out that your credit cards were maxed out while you slept.

And a few weeks later, the IRS contacts you for an audit, because your Social Security number was used to commit tax fraud.

What a nightmare! I know people who have gone through it, and it can take years to unravel. You have large legal bills, difficulty in reestablishing good credit, and a lot of money is gone forever.

This is all avoidable; and this e-book will show you exactly how to stop email hackers cold in their tracks. You'll learn ...

- ** Why the two most often purchased anti-virus programs, McAfee and Symantec, can't protect you from email scams
- ** Five FREE anti-virus programs that are better, and where and how to download them
- ** Why the popular Internet Explorer has long been a sieve for viruses and malware to enter your computer
- ** Two popular Internet Browsers that give you much better security

- ** The dirty trick producers of “free” software use to get paid
- ** Do you have a router? If you don’t protect it with passwords (not one, but two), a hacker can drive by in a van, get into your computer by the router and steal all your passwords and login info to your bank, pharmacy, insurance companies, credit cards, eBay, and other online shopping sites
- ** How the Supreme Court recently ruled that anyone can snoop your computer WITHOUT a warrant — if your WiFi isn’t password protected
- ** How to create a password that hackers couldn’t crack in centuries
- ** How Trump’s White House is protecting its communications from disasters like Hillary’s email. It’s software that Edward Snowden recommends and is using.

Part 1 of this e-book covers email safety and the hack that undid Hillary campaign manager John Podesta.

Part 2 shows you why it’s essential to secure your router as well as your computer, and how to do each.

Part 3 covers how the government can be as big a threat to your computer security as hackers, and how to combat it.

Part 4 gives simple, reliable strategies anyone can use to protect your email against hackers. We also show you how to stay updated against new threats from hackers and the government going forward. It’s FREE. ♦

Table of Contents

Part I Email safety and the hack that undid John Podesta

Chapter 1	1
<i>Email security: What difference does it make?</i>	
Chapter 2	1
<i>Leaked emails</i>	
Chapter 3	2
<i>How does this affect you?</i>	
Chapter 4	2
<i>The hack that tripped up John Podesta</i>	
Chapter 5	3
<i>Getting started</i>	

Part II Computer and router security

Chapter 6	7
<i>Use an antivirus program</i>	
Chapter 7	7
<i>Why uninstalling McAfee or Symantec anti-virus could be the right move</i>	
Chapter 8	8
<i>Installing a better anti-virus program — for free!</i>	
Chapter 9	9
<i>Use a browser with built-in browsing safety</i>	
Chapter 10	10
<i>Microsoft's browsers</i>	
Chapter 11	11
<i>The dirty trick that pays for “free” software</i>	
Chapter 12	13
<i>Set up WiFi passwords on your wireless router</i>	

Part III

Your computer and the government

Chapter 13	17
<i>No router password, no privacy.</i>	
Chapter 14	20
<i>How to keep your messages secure and private — even if your computer and router aren't!</i>	
Chapter 15	21
<i>The greatest threat to your privacy won't come from a hacker</i>	
Chapter 16	25
<i>When even the most secure app in the world can't keep your secrets safe</i>	
Chapter 17	27
<i>How you can protect your privacy from warrantless spying by the government</i>	

Part IV

Protecting yourself from email hacks

Chapter 18	35
<i>Use strong passwords for your email accounts</i>	
Chapter 19	36
<i>How a hacker cracks your password</i>	
Chapter 20	39
<i>The best password is the one that takes the longest to crack</i>	
Chapter 21	44
<i>How to generate strong passwords</i>	
Chapter 22	47
<i>More password dos and don'ts</i>	
Chapter 23	47
<i>Answering the so-called "Security Question": Lie!</i>	
Chapter 24	48
<i>You have to tell these programs to encrypt your email</i>	

Chapter 25	51
<i>Types of email accounts and what Outlook needs to use them</i>	
Chapter 26	53
<i>POP3 or IMAP?</i>	
Chapter 27	53
<i>Port settings and TLS/SSL</i>	
Chapter 28	54
<i>Why you should avoid cable provider email accounts</i>	
Chapter 29	56
<i>Use “two-factor authentication” for your online email accounts if you’re a privacy fanatic</i>	
Chapter 30	58
<i>The email hack that scuttled Hillary’s presidential hopes</i>	
Chapter 31	61
<i>Is that email really a phishing scam?</i>	
Chapter 32	63
<i>How to spot what John Podesta and Hillary’s IT team missed</i>	
Chapter 33	67
<i>Stay protected and up-to-date as new threats emerge</i>	

Part I

Email safety and the hack that undid John Podesta

Chapter 1

Email security: What difference does it make?

Bad email security cost Hillary the presidency.

Hillary can blame FBI Director James Comey, she can blame the Russians.

But the fact of it is, the flames that set off the powder keg under Hillary's campaign were fanned by her campaign's lack of email security.

From her careless use of a private email server ... to leaked emails stolen from the Democratic National Committee ... to more leaked emails stolen from campaign chairman John Podesta's account, hundreds of damaging emails exposed the ugly truth that roiled beneath the surface of Hillary's campaign: Lies. Collusion. Sabotage. Influence-peddling.



Is Comey to blame for Hillary's lousy email habits?

Chapter 2

Leaked emails

Leaked emails proved that Hillary lied about her private email server — how it was used, what was on it, and what she deleted from it.

Leaked emails proved that foreign donors funneled cash into the Clinton Foundation in exchange for preferential access to State Department officials.

Leaked emails proved that members of the media worked with Hillary's campaign to shape their pro-Hillary reporting and hone their anti-Trump narrative.

Leaked emails proved Bernie Sanders was right when he accused the DNC and Hillary of conspiring to elbow him out of the race for the nomination.

Until the emails were leaked, people thought Bernie was just a crazy old commie, waving his hands in the air and spewing paranoid nonsense. After the leaks, the DNC lost all credibility as being anything but a campaign office for Hillary.

The leaked emails, being nothing but electronic data, had no physical weight. But they sank Hillary's campaign as surely as a battleship anchor would sink a lifeboat.

It's too late for her now, but had she and her campaign taken email security a little more seriously, the 2016 election would have had a very different outcome.

Chapter 3

How does this affect you?

Look, you might not need to cover up the activities of a multi-million-dollar family foundation that acts as a cash funnel for foreign donors who want access to the State Department.

But on a practical level:

- You don't want your identity stolen,
- Your bank account emptied,
- Your credit cards ringing up purchases you didn't make, or
- IRS agents knocking at your door because your Social Security number was used to commit tax fraud.

Repairing your finances and reclaiming your identity after it's stolen in a hack can take months, even years. Protecting your computer from getting easily hacked in the first place takes an hour or two at most.

In this e-book, I'm going to show you how you can protect yourself from the kinds of hacks that crippled Hillary's campaign.

Chapter 4

The hack that tripped up John Podesta

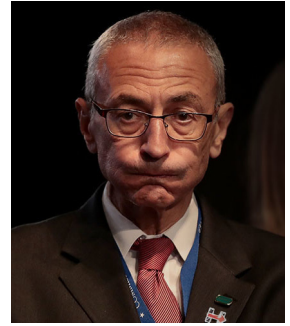
Hillary's campaign chair, John Podesta — whose emails

were plastered all over the internet thanks to WikiLeaks — fell for one of the scams I'll show you how to avoid below, called phishing.

Even Hillary's IT staff completely missed the signs of the phishing scam, and their carelessly-worded memo to Podesta sent him right into the hacker's trap.

His ignorance — and their poor communication skills — cost Hillary the election.

Even if you're not running for President of the United States, by the time you finish reading this e-book you'll know how to identify and avoid email hacking scams better than Hillary's campaign did.



John Podesta:
Poster child of email
hack victims.

Chapter 5

Getting started

Many people know that email security is important — but they don't know what they need to do to get it, or where to start.

They just leave their computer and programs running with the same settings as the day they first got them, and hope for the best. It doesn't take much to hack a system that's completely unprotected like that.

Do you think you're protected from hackers because you use an antivirus program like McAfee or Symantec?

Think again. The email hack that took down Hillary's campaign slipped right past Podesta's antivirus program. It didn't stop him from opening the malicious — and fake — email, and it didn't stop him from clicking the link to the hacker website that stole his Gmail login.

Each of the security measures on these pages will make your computer less likely to get hacked. The more of these you use, the stronger your security will be.

Naturally, you can't completely prevent email hacking, any more than you can completely prevent crime. Crime is going to happen.

That said, would you walk through gang territory in Chicago,

alone, at 2:00 AM? Of course not. That would be foolish and just asking to be robbed, beaten up, or killed. Or all three.

No. You'd be careful not to be an easy target for thieves, thugs, and killers. You would stick to well-lit, well-populated streets during the day. You would walk in a group of people when you could. You'd keep your money out of reach from a pickpocket. You'd walk briskly and with purpose, and above all, you'd be aware of what's around you. All common-sense stuff.

Likewise, you can't prevent a hacker from trying to hack you. But you don't have to roll out the red carpet for them. Your job is to make it hard for them to victimize you. Hacking is a crime of opportunity. Most hackers will give up after a few unsuccessful attempts. When that happens, you win! ♦

Part II

Computer and router security

Chapter 6

Use an antivirus program **(Difficulty level: Easy)**

Having secure email won't be of much use if hackers can steal your passwords and login info from right under your nose by logging into your unprotected wireless router or computer. So take these simple steps to make sure those are secured.

Hackers plant computer viruses that can secretly record all the data going into and out of your computer. This includes your banking logins, your social security number, your credit card numbers, your medical logins — anything you do online, the hacker knows.

There is no excuse to not use an antivirus program on your computer.

Most computers come preloaded with either McAfee and Symantec, which are two very popular choices.

Chapter 7

Why uninstalling McAfee or Symantec anti-virus could be the right move

“Most popular” doesn't always mean “best.” Under certain conditions, McAfee and Symantec can cause your computer to act up so badly you might think you have a computer virus. Common problems include having your system freeze up or crash for no reason, or taking forever to load a program.

If this is happening to you, you might want to uninstall McAfee or Symantec, and install one of the excellent FREE antivirus programs instead.

I've had to uninstall McAfee or Symantec from four computers over the past year, because the computers were slowing down and crashing for no apparent reason. I installed a free antivirus program in their place (see below), and the computers ran normally again — the slowdowns and crashing went away.

Because of the way McAfee and Symantec work, you can't just uninstall them from the Windows Control Panel. Instead, do a Google search for "how to completely uninstall McAfee on Windows 10" (or whatever anti-virus program and operating system you use) and download one of the uninstaller programs available for them.

Chapter 8

Installing a better anti-virus program — for free!

The [BitDefender site](#) has a list of antivirus uninstallers for many popular programs.

Once you've removed McAfee or Symantec, download and install any one of the free antivirus programs listed in this [Tech Radar article](#). If you can't decide, I recommend Avast Free edition. That's the program I use, and the one I replaced McAfee and Symantec with, on those four wonky computers.

The internet is a fast-changing place, and clever hackers are constantly coming up with new scams. To get free updates to this e-book, email us at freeupdates@renegadeadvisory.com, or phone Ella at 1-866-500-6746.

Tip: Don't bother installing all the optional "extra protection" doo-dads that Avast offers you. Most of the extra features won't work unless you pay for them, and you don't need them, anyway. Uncheck items like the software updater, secure browser, system cleanup, sandbox, and any of that other stuff. Just select anti-virus protection for files and e-mail, and that's about all.

The free Avast program will display small pop-up notifications in the corner of your screen periodically, and most of them are ads for extra-cost items. You can simply dismiss the notifications.

The program will automatically update its malware identification database every few hours, giving you maximum protection against malware. If you're using a different anti-virus program, be sure that it also updates its database frequently.

Chapter 9

Use a browser with built-in browsing safety

(Difficulty level: Easy)

Are you still using Internet Explorer on a Windows XP computer? If so, you're practically a sitting duck for a hacker. Windows XP is long past its expiration date, and Internet Explorer has long been a sieve for viruses and malware to enter your computer.

Did you know there are at least a half-dozen major browsers that run on Windows that are better than Internet Explorer? And they're all free!

We'll keep it simple and stick with the top few picks.

Recent versions of Google Chrome and Mozilla Firefox will warn you if you attempt to visit a website that is known to download viruses or contain phishing scams (tricks to get you to reveal your logins). These are an important front-line defense against email hacks.

► **Google Chrome** (Windows, Mac, Android, iPhone, iPad, Linux)

Chrome is the top-rated browser in many rankings, because it's fast, stable, has lots of available extensions, and can warn you if you try to visit a harmful website that might download malware onto your computer.

Chances are, if John Podesta was using a recent version of Chrome, it would have warned him that the website link he visited was dangerous.

I recommend you install Chrome as your go-to browser. Chrome can be installed on just about any operating system (Windows, Mac, Linux, iOS, Android), and you can sync settings like your bookmarks (a.k.a. Favorites) and extensions (a.k.a. plugins or addons) between your tablet, smartphone, and computers.

Chrome works best on newer computers (less than three years old) with lots of RAM (8 GB or more). Having too many Chrome tabs open at once can cause older computers to slow down or freeze.

► **Mozilla Firefox**

Firefox used to be the king of the browser hill, until Chrome stole the crown. But Firefox is still a capable and secure browser that is worth a look. It too has a wealth of extensions that can give it all sorts of capabilities beyond a plain-vanilla browser.

Firefox is a good choice if you have a much older computer that chokes when it tries to run Chrome.

► **Safari** (Mac)

Chrome, my preferred browser, can be installed on a Mac. But Safari, the browser that comes preinstalled on Apple computers, has features that integrate specifically with the Mac. So if you want to stick with Safari, no worries — it's a solid browser that will give you top-notch security and performance on Apple devices.

(There used to be a version of Safari that ran on Windows, but that version hasn't been updated since 2012, so it doesn't have protection against modern web hacking techniques. The outdated versions of Safari for Windows are still floating around online, but don't install them!)

Chapter 10

Microsoft's browsers — Edge: use it if you want. IE: never, ever use it

► **Microsoft Edge** (Windows 10 only)

Edge is the built-in browser for Windows 10. It's an okay browser — it's not the security nightmare that Internet Explorer is — but Edge only runs on Windows 10, nothing else. If you want to use it on your iPhone or Android phone, or on any non-Windows tablets — or even on Windows 7 — you're out of luck!

But you can install Chrome or Firefox on just about anything: your iPhone, Android phone, iPad, Android tablet, your Mac, and your PC. That means you'll have a consistent browser experience on all your devices — which might save you some frustration!

So if you spend most of your computer time on a PC with Windows 10, Edge is okay. But if you want a browser that can do more than just basic web surfing, I recommend you install Chrome or Firefox as your go-to.

► Internet Explorer

I'll make this simple. If you're using any version of Internet Explorer, **stop using it**. Right now. Install Chrome or Firefox instead.

Microsoft has discontinued support for all versions of IE except for the most recent, IE 11. That means no bug fixes, no security updates, nada, nothing, zip.

Even IE 11 will eventually be discontinued in favor of the Windows 10 Edge browser (see the next item). So the longer you cling to IE, the more vulnerable you're making yourself to hackers.

Chapter 11

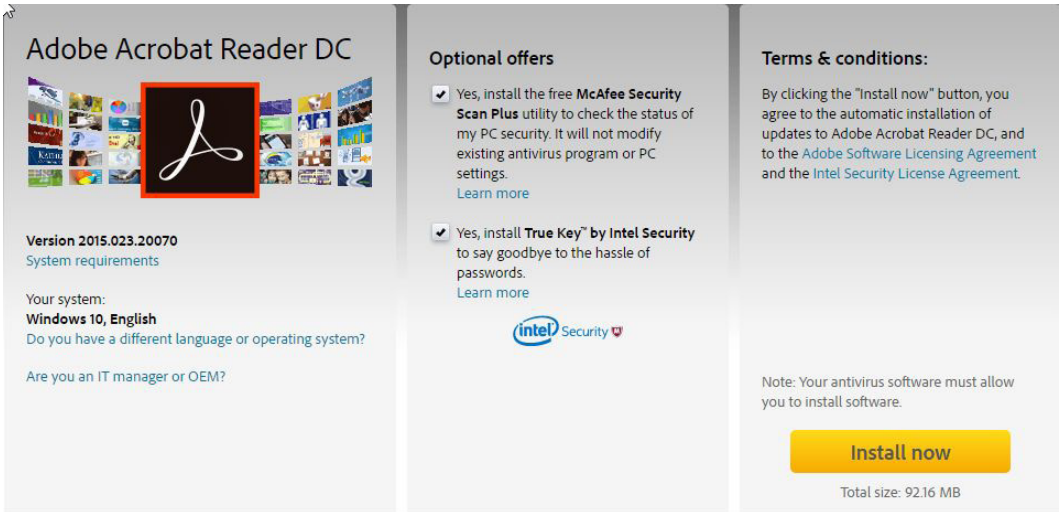
The dirty trick that pays for “free” software or, Don't automatically click Next when you install a new program (Difficulty level: Easy to Medium)

Free programs can be awesome. You often get features that rival their more expensive commercial counterparts, but at no cost.

Well, almost no cost. To make any money giving away free software, many publishers add screens to their installation programs that trick you into installing additional unwanted programs — called crapware. They get paid for doing this.

While technically not viruses, crapware can make a mess of your system by changing some of the default programs and preferences you have. The next thing you know, your browser home page has been changed, and you don't know how that happened. You suspect a virus, but it's probably just crapware that you accidentally installed.

The installation screens for crapware are written to confuse you because they make it look like the crapware is a recommended option for the program you're installing. But they're not.



Adobe software should be safe to download, right? Not so fast! Don't click that big yellow **Install Now** button until you **UNCHECK** the crapware downloads in the middle panel that Adobe has selected by default! Shame on Adobe for tricking millions of users into downloading unwanted crapware.

And the checkbox that accepts the crapware is **ALWAYS** checked by default, which means you'll install the crapware unless you specifically decline it. And to make it even more slimy, the option to decline the crapware is often **GRAYED OUT** to make it appear as if it's disabled (it's not; you can still click it to decline).

Even programs from major software companies like Adobe add crapware to their installations — and the crapware is selected by default! One is McAfee Security Scan Plus ... a program that can seriously mess up your computer.

So read the fine print carefully on the installation screens. Look for checkboxes or selection buttons on every screen. If you see any reference to a program that isn't what you wanted to install, select **DECLINE** or **I DO NOT ACCEPT** or **NO THANKS** or **UNCHECK** or whatever button or checkbox means **NO**, before you continue.

The How-To Geek has a pretty comprehensive inventory of [crapware screens](#) that different software websites add to their programs. If you see any installation screens that look like those, pay attention and decline them!



Chapter 12

Set up WiFi passwords on your wireless router

(Difficulty level: Medium)

Many people assume that the password they use to get WiFi is the only one they need to set in their wireless router.

This might be true if your cable provider gave you a router with WiFi built into it. If you only have a cable modem and nothing else attached to it, you can probably skip this section.

But if you have a separate WiFi router connected to your cable modem, read on.

If you have a router, it's likely a popular brand like Cisco/Linksys, Netgear, D-Link, Belkin, TP Link or Asus.

If you have one of these, there are two passwords — yes, two — that you need to set.

The first is the Administrator password for the router's control panel. The Administrator password is separate from your WiFi password. The Administrator password is for logging in to the control panel that lets you change the router's settings.

By default, many brands of routers have ridiculously simple Administrator logins (like a



Wireless routers come in all shapes and sizes. But no matter how many antennas they have, you need to change *two passwords* to protect your WiFi from hackers.

username of “admin” and a password of “password”) that make your router dead-simple to hack unless you change them to something else.

This is a serious issue because some routers allow an administrator to log in and make changes to the router over the internet. If you don’t change the default Administrator password, a hacker can easily Google it and take control of your router — and steal all your passwords and login info to every site you visit: bank, pharmacy, insurance, credit card, shopping, taxes, you name it.

The second is the password to log in to your internet’s WiFi. This is your WiFi password — it’s the password you give to your kids when they come to visit and want to get on the internet with their phones and computers.

At least I *hope* you need to give them a password.

Do a factory reset to protect your router against VPNFilter malware. In 2018, security experts discovered a nasty bit of Russian malware dubbed *VPNFilter*. While most malware infects personal computers, this malware attacks your WiFi router, which puts it beyond the reach of the anti-virus program running on your PC.

VPNFilter can give a hacker complete control over all internet traffic that goes through your WiFi router — passwords, account information, and other personal data — without you knowing it. And it can steal data from *any device* connected to WiFi, not just your PC.

This malware can send fake web traffic to your computer that looks like you have a normal bank balance, when in fact your bank funds are being transferred to a hacker’s account right under your nose. You won’t know you’ve been hacked until your checks and online payments start bouncing.

The only protection against VPNFilter for now is to perform a “factory reset” of your WiFi router. On the back of your router (or the bottom, on some models) will be a small pinhole typically labeled “RESET.”

Insert a paper clip into this hole and depress it for 30 seconds before releasing. This will completely erase your router’s settings back to the original, factory state — and delete VPNFilter along with it. After you’ve done this, be sure to set brand new Administrator and WiFi login passwords for your router. ♦

Part III

Your computer and the government

Chapter 13

No router password, no privacy. The police or anyone can snoop WITHOUT a warrant

Many of the newer routers force you to create a WiFi password when they're first set up, and you can't ignore it. That's good. But some older routers didn't force you to create a password for WiFi, which is bad.

Without a WiFi password, a hacker driving by in a van can record everything your computers are doing by connecting to your wireless router from the street, easy-peasy. Their computer will even tell them your router is UNSECURED. Ka-ching — goodbye bank account!

Even worse, not protecting your router with a password could make hacking the least of your problems — you could actually be giving up your Fourth Amendment right to privacy!

Courts have ruled that “it is entirely lawful to snoop in on someone else's private communications over an unsecured wireless network.”

An unsecured router means you forfeit any expectation of privacy, because your WiFi signal is considered “readily available to the general public.”

The police can copy files off your computer through your unprotected WiFi router, and any evidence they find can be used against you in court. Maybe even without a warrant. Are you willing to take that chance?

And if the creepy neighbor next door connects to your unprotected WiFi router and distributes child porn from it, you could find yourself face-down on



Police SWAT teams have raided the homes of unsuspecting citizens whose unprotected WiFi was used by their neighbors to commit online crimes.

One home in Indiana was invaded by 11 SWAT cops who smashed the door and windows in, and tossed flashbang grenades into the house before entering.

Inside, the cops found a 68-year-old grandmother and her adopted daughter. They ordered the women to the floor, handcuffed and arrested them, then took them to jail in a police van. The two women were innocent.

the floor, rifles trained on the back of your head, with a SWAT team shouting at you to “STAY DOWN! STAY DOWN!” as they seize your computers and ransack your home.

This is not some fictional scenario I made up. **It’s already happened — more than once.**

If you don’t have a WiFi password, or aren’t sure if you do, you need to fix that situation pronto.

If you’ve bought a new computer in the past several years, but you’re using the same WiFi router you’ve had since who-knows-when, consider buying a new router now. A good router costs under a hundred bucks, but that’s peanuts compared to what you could lose if your old router isn’t up to snuff with today’s security standards.

An added benefit of a new router is that your web browsing might be speedier. Nowadays, computers aren’t the only thing that need WiFi: your tablets, phones, TVs, DVD player, video game system, Amazon Alexa, home security system — maybe even your thermostat or light switches — are all clamoring for their slice of your WiFi signal. An older router can’t deal with the extra traffic very well.

If you don’t know what brand and model wireless router you have, go over to it and pick it up. Look for a label somewhere on it. Look



underneath, in back, on top, on the sides. There will be a label somewhere on it with the brand and model number.

Write down the router’s brand and model number — or take a picture of it with your phone, like I do.

Sometimes manufacturers clearly identify the model number on their labels. Other times, they make you hunt for it, like this Netgear router does.

Tip: The model number is usually at the top of the label under the brand logo. Almost all model numbers are **2 or 3 letters** followed by **3 or 4 numbers** — sometimes followed by a couple more letters.

Did you spot the model number on this label? If you said **DGN2000**, you’re right!

Next, we want to find out how to change the passwords on the router. If you have the user guide for your router handy, follow that. Most of the time,

though, the user guide — if you ever had it — will have disappeared long ago, so we'll have to turn to Google for help.

**NOTE**

The instructions that follow are for the router shown in the example photograph on the prior page, which may not be the same as your router. You will need to adapt the instructions for the brand and model router you have instead. Your search results will differ as well.

We'll use the router pictured in the photo on the previous page for our example. According to the label, this is a Netgear model DGN2000 (your router model will likely be different). Search Google for “change passwords on Netgear DGN2000 router.”

You'll get a lot of search results. If you're not sure which link has the instructions you want, visit each of them until you find a website whose instructions you can understand and follow. (Skip the search results that say “Ad” next to them.)

When we look at the search results for the Netgear DGN2000, we see a link for [DGN2000 Manual: How to Change the Built-In Password - Netgear](#). Visiting that page, we see that these are the instructions to change the router's Administrator password, which we discussed in the previous chapter.

But remember, there are two passwords to change, and you need to find the instructions for both. We look through our search results again, and find a link for [Smart Wizard - How to change your NETGEAR router WiFi password](#). From the title, we know this is the WiFi login that we also mentioned in the previous chapter. So we now know how to set both passwords in our hypothetical example.

If you've gone through a page or two of search results and they all seem too technical for you, try adding the word “beginners” to the end of your search phrase and try again.

(NOTE: Don't use a wimpy, easily-hacked password on your router. Read about how to select a secure password in Chapters 20 and 21.)

The internet is a fast-changing place, and clever hackers are constantly coming up with new scams. To get free updates to this e-book, email us at freeupdates@renegadeadvisory.com, or phone Ella at 1-866-500-6746.

Chapter 14

How to keep your messages secure and private — even if your computer and router aren't!

What if the most secure email is ... no email?

Don't scoff — that's not as ridiculous as it might sound.

According to the Wall Street Journal, aides to President Trump are ditching their hack-prone email, and are using an app called Signal to safeguard their messages from hacking.

Signal is an ultra-secure messaging app lauded by cyber-security experts. Its state-of-the-art encryption technology ensures that private messages stay hidden from hackers or spy agency snoops. It's like Skype on security steroids.

Roger Stone, one of the president's closest aides, told the Wall Street Journal he started using Signal last fall after an email hack left him picking up pieces of his life. Stone watched helplessly as 30 years of contact information was wiped out and his personal and business bank accounts were compromised.

"I learned my lesson," Stone said. "It was hell. I realized I needed a safer encrypted way to communicate—and NO I have never communicated with any Russians on Signal."

The Trump Administration isn't alone in favoring Signal over email. Politicians at every level, in both parties, are turning to it as well. Signal has quietly become the go-to messaging app among politicians who want to avoid waking up one day to their emails posted all across the internet by WikiLeaks.

Democratic National Committee leaders ordered their staff to stop using email and use Signal instead, after a scandal erupted over leaked emails that proved the DNC was in cahoots with Hillary. The emails revealed staffers actively discussed ways to sabotage Bernie Sanders' campaign during the primaries, to clear Hillary's path to the nomination.

Even Hillary — who feigned cluelessness when questioned

about her private email server — grew tech-savvy real quick after her campaign was rocked by a spate of explosive email leaks. She too ordered her staff to cease using email for sensitive messages and use Signal instead.

Using Signal probably prevented future email hacks, but Hillary was closing the barn door after the horses had already bolted. Two months before her edict, campaign chair John Podesta fell for an email phishing scam that tricked him into giving hackers his Gmail login and password.

The huge booty of 50,000 emails plundered from Podesta's account showed up on WikiLeaks later that summer. Their bombshell revelations torpedoed Hillary's campaign and immortalized Podesta as the poster child for hacking victims.

Chapter 15

The greatest threat to your privacy won't come from a hacker

Email hacks are destructive, yes, but you face a far more insidious threat to your privacy. For years, a state-sponsored actor has been compiling a dossier on you with every tweet, text, phone call, Instagram photo, and Facebook post you make.

The threat isn't coming from Russia, China, Iran, or even North Korea.

In 2013, NSA contractor Edward Snowden released a treasure trove of classified documents to the press that proved the NSA had been conducting sweeping surveillance programs of US citizens and foreign leaders — secretly tapping their email accounts, instant messaging records, and phone records.

In some cases, a secret court order forced companies to comply with the NSA's demands. Where no court order was available, the NSA went ahead anyway and tapped the undersea cables that carried Yahoo and Google internet traffic, siphoning data from millions of accounts.

(Snowden currently lives in Russia under temporary asylum, after the US government revoked his passport.)

Hillary insisted her staff use Signal because it was “Snowden-approved” — an ironic nod to his authority on privacy, since she considered the NSA whistleblower a traitor who should be prosecuted and imprisoned.

Snowden avidly endorses the Signal app, and praises its ability to hide private messages from the far-reaching surveillance clutches of the government.

Signal may be your best protection against warrantless wiretapping by the NSA ... CIA ... FBI ... IRS ... and local police departments that secretly use [Stingray](#) or [Triggerfish](#) eavesdropping devices to intercept your calls and messages without your knowledge — and without a court order.

[Signal is FREE](#), and is available on iPhone from the App Store, on Android from Google Play, and on Windows as a [Google Chrome extension](#).

The Chrome extension for Windows requires you to install Signal on your smartphone first, but once you do, you can send and receive secure Signal messages right from your PC.

Signal is dead-simple to use. The app hides all of the complexities of cyber encryption under the hood, and deliberately keeps the interface bare-bones by limiting the number of options you need to choose.

Their goal was to roll advanced, secure messaging into the simplest interface possible. They’ve succeeded.

As if high-grade encryption weren’t enough, you can also tell Signal messages to self-destruct after the recipient views them.

The self-destruct delay can be set from 5 seconds to one week, and the recipient cannot stop it. This ensures no trace of your private messages can be carelessly left behind for pilfering by hackers.

For example, you can use Signal to send your garage entry and home alarm codes to a visiting family member if you’re not at home to let them in, and make the message automatically disappear 10 minutes after they view it.

It’s safer than sending the codes via email, where your codes

would be viewable by others long after they were used, and safer than a plain text message, which could be intercepted and read by an eavesdropping device.

You can also make secure, encrypted phone calls to other Signal users. Unlike standard phone calls or Skype calls, Signal calls cannot be deciphered and played back if they are intercepted.

Signal takes security a step further by warning you if someone is hacking the connection between you and the other caller.

On each call you make, the app displays a two-word “trust phrase” on the screen that you and the other caller both see.

If all's well with the connection, and your messages are not being intercepted by a hacker who is listening in on an insecure WiFi connection, you'll both see the same the trust phrase. Confirm it with the other caller before you begin your conversation.

But if a hacker secretly inserts himself in the middle of the connection, you and the other caller will see different trust phrases.

If that happens, the connection has been compromised and it's not safe to talk. You should hang up and try calling from a different WiFi location.

Signal also has secure group chats, so several people can hold a conference, and a hacker who somehow tapped the line would be unable to read or hear the messages flowing back and forth between the group.

And Signal now has encrypted video calls, similar to Skype video chat. The big difference is that Signal's secure video calls cannot be deciphered and viewed by anyone not on the call.

Other messaging apps offer secure chats as an option — Facebook Messenger and WhatsApp among them — but security is turned OFF by default, leaving your messages vulnerable to eavesdropping and hacking. You have to go in and change the settings to get security to work in them.

What's more, those apps send their meta-data through Facebook servers — snippets of data that can be used to identify and track you.

And worse, security experts warn that your contacts and message

history are backed up to the cloud if your phone does automatic backups, which almost all of them do. Cloud servers are vulnerable to hacking and data theft.

Security experts love Signal because strong security is baked into it from the get-go.

Signal's high-security mode is permanently on, protecting your messages the instant you open the app. The tiny slivers of meta-data it sends is not saved on any servers.

Signal is ultra-secure because none of your data needs to pass through an intermediate server, like Skype chats do. Everything you say or send to the other caller is completely encrypted and vice-versa.

Even if your phone makes automatic cloud backups, only the Signal app and your Signal contact list will be backed up — but the contact list will be encrypted and safe from hacking.

Plus, Signal is somehow able to prevent your phone from backing up your encrypted messages at all. It's like they're protected by a cloaking shield that makes them invisible.

And finally, Signal has created a way to let users carry on conversations *even if the app is banned or blocked*, as it has been in certain Middle East countries. This feature has the potential to open the floodgates to the uncensored exchange of ideas around the world.

Signal evades blocks by making its data traffic masquerade as an innocuous Google search. So unless Google has been blocked outright (and sometimes countries like Syria do that), there's no way for government servers to identify Signal calls, much less prevent them from going through. Signal's data traffic is hidden among the billions of Google search queries made every day. Ingenious!

So even if you visit a country where internet traffic is routinely monitored — either to crush dissent or to enforce draconian laws that criminalize free speech — Signal lets you chat freely by voice and text with any of your Signal contacts, without fear of running afoul of censorship laws.

Protecting individual privacy where none exists is a lofty ideal — much less for an app — but Signal does it with aplomb.

Last year’s presidential election made the brutal consequences of poor email security painfully clear. Safeguarding the privacy of messages has taken on a new urgency for everyone who uses chat or email — politician or not.

Not surprisingly, downloads of Signal are up 400% since Trump’s election.

Even if you’re not ready to give up email entirely, it makes sense to protect your privacy with Signal, beginning today.

As one political operative told the Wall Street Journal, “No one wants to end up like Podesta.”

Chapter 16

When even the most secure app in the world can’t keep your secrets safe

Signal is the most secure messaging app in the world. The messages you send to someone with Signal can’t be decrypted if they are intercepted. Not even the CIA or NSA is able to crack Signal messages once they’re transmitted.

Since cracking Signal is an unwinnable battle for the foreseeable future, these agencies have shifted their cyber-espionage attention to your phone itself — finding ways to spy on you as you use it, according to internal CIA documents leaked by WikiLeaks.

If the cyber-spooks can trick you into installing malware onto your phone that sends all your keyboard inputs to their servers — or silently takes screenshots every few seconds, or secretly records your voice audio — they don’t have to decrypt anything.

They can record *everything you type, view or say as you do it*: your login passwords, love notes, text messages, and yes, any confidential messages you type up in Signal before you hit Send.

This category of malware — dubbed “spyware” — was one of the earliest forms of hacking on PCs, and gave rise to the entire anti-virus software industry.

Hackers would infect PCs with “keylogger” viruses that sent



The CIA has collected a massive library of security weaknesses in consumer electronic devices and software, and they've created programs that exploit those security holes to infect a computer, phone, or TV — turning them into spy cams, room bugs, or screen recorders right under the owner's nose.

hackers everything a user typed on his computer. The CIA and NSA have simply appropriated that hacking technique and applied it to smartphones.

The 8,700 CIA documents released by WikiLeaks describe, in chilling detail, the software that the CIA, NSA, and British Intelligence are developing to turn our phones, TVs, and computers into government-controlled bugging devices that can be used against us.

One of their programs exploits a gaping security hole in some models of Samsung TVs that allows the CIA to turn the TV into a room bugging device, picking up conversations through the TV's built-in microphone even though the TV appears to be turned off.

This particular form of malware has to be physically installed on the victim's television set from a USB thumb drive. This could be done without a trace by surreptitiously breaking into the victim's home when he is away, or in the presence of the victim by an agent posing as a cable service technician.

Other CIA software infects computer operating systems from Microsoft and Apple, as well as iPhones and Android smartphones.

For the CIA to control a phone, the phone's owner has to be tricked into installing the malware (probably by opening an infected file attachment), or an accomplice has to install the malware when they

have access to the phone. Do you leave your phone unattended with your paramour or acquaintances? You're at risk.

The fact that the CIA and NSA have to install malware on your phone — by hand, in person — is a validation of Signal's effectiveness.

But it's also a reminder that there are many avenues — “attack vectors” in security parlance — the government can use to get at your communication.

After Edward Snowden's 2013 release of classified NSA documents detailing its widespread digital surveillance programs, then-president Barack Obama pledged to inform US software makers of any security vulnerabilities the government discovered in their software.

However, the leaked documents show that the CIA has been hoarding a vast library of security vulnerabilities for their own use against software makers, despite what Obama promised.

In retaliation, Julian Assange, founder of WikiLeaks, has promised to give major technology companies exclusive access to the CIA's programming source code (which he has not yet made public) so the companies can study the code and patch their systems to defend against those attacks.

Chapter 17

How you can protect your privacy from warrantless spying by the government

The NSA leaks from Snowden, and the more recent CIA leaks from unnamed sources make it clear that government intelligence agencies are conducting an ongoing assault against individual privacy by attacking the electronic devices we use every day.

Security experts admit that if the government targets you for surveillance, there's not much you can do to stop it. They have limitless resources at their disposal, and you don't.

The only way to ensure your personal electronics aren't compromised by government spyware is to turn them off, melt them down, and live offline and off-grid. That's an extreme option that

doesn't suit most people.

A simpler, more pragmatic approach is to ***never say or write anything on an electronic device that you don't want recorded by the government.***

In the bleak, soul-crushing world of extreme paranoia the intelligence community lives in, what you consider to be free speech the government may consider to be sedition.

Even if the risk of government surveillance isn't high on your list of worries, you need to take steps to ensure your devices aren't putting out the welcome mat for malware infections.

- ▶ Use anti-virus security software on your PCs and phones. We talked about the excellent free security programs available for PCs in an earlier chapter.

There are also many excellent, free security apps available for iPhones and Android phones. Check the Apple Store or Google Play Store for your phone. Install one and keep your phone protected.

I use CM Security by Cheetah Mobile — it's a free, feature-packed security app for iPhone and Android phones. In addition to excellent malware protection, it has an app locker that can protect individual apps with a PIN number, a call blocker that can warn you of incoming telemarketing calls before you answer, and a safe browser that will warn you of phishing websites and delete all your browsing history when you close it.

- ▶ Keep the software on all of your phones, computers, and TVs up-to-date. Ditto for game consoles, smart home appliances and switches. Even your WiFi router! Anything that uses WiFi is a potential entry point for malware, and needs to be updated regularly. If you don't want to do this, then unplug your router and stay offline.
- ▶ Old equipment that no longer receives security patches should be replaced with newer models. Again, your WiFi router is a place to start. Replace it if it's more than five years old.
- ▶ Any Windows computer not running Windows 10 is also ripe for upgrade — I know many people still love and use Windows 7, but Microsoft is phasing it out in a couple more years. Don't

let your resistance to change turn you into a hacking target.

- ▶ Look at your smartphone: is it more than three years old? The software on it is probably a few versions behind the current version, and is no longer updated. That puts you at a higher risk of being hacked. It's time to get a new phone!
- ▶ Turn on automatic updates on your devices, so security patches are installed immediately upon release. Go to Google, type "enable automatic updates for _____" and fill in your phone, tablet, or PC model.

Security experts believe that some of the CIA's exploits are specifically designed for older versions of software residing on the devices they're meant to attack — and updating the devices' operating software with the latest security patches can make the malware ineffective.

Indeed, companies like Apple and Microsoft believe that the most recent updates of their software already protect their devices against many of the hacks revealed in the CIA documents.

The CIA is counting on the fact that many people don't take the time to regularly update their software, if they do it at all. And while it's certain that the cyber-spooks are updating their malware programs to infiltrate newer versions of devices, some of their older programs will work as-is on devices that haven't been updated.

Spying vs. privacy, and hackers vs. security, is a constant cat-and-mouse game, and for most people, the cats always seem to have the upper hand.

As bleak as this landscape sounds, you *can* communicate electronically and keep your messages private — but you have to take extreme measures to keep your secrets hidden from government spies. It requires you to be as technically adept as the spies themselves.

Until Snowden revealed to the world — from his Hong Kong hotel room in 2013 — that he was the man responsible for leaking the NSA files, the agency had no idea who the leaker was, where he was, or how he managed to stay hidden from them for so long.

How did Snowden thwart the NSA's nearly-omniscient surveillance and tracking capabilities? And not just Snowden, but the reporters he collaborated with? How did everyone involved with the



In 2013, Edward Snowden blew the lid off a massive operation of covert, warrantless spying on Americans by the NSA. He stayed safely hidden from the NSA's cyber-manhunt by communicating on a laptop that ran TAILS, an operating system that cloaked all of his online activity.

leaks manage to give the NSA the slip — until they revealed themselves?

They communicated via laptops running a super-secure operating system called TAILS. It's a custom-designed operating system that requires technical know-how to install and configure — and use.

Its main feature is that it lets you go online, and not be identified or located by your IP address. TAILS connects to the internet through TOR, a hyper-privacy network that hides your true IP address and replaces it with an IP address that can't be traced back to you.

TAILS is like the Signal app, but for an entire computer system. If you communicate with another person who is using a TAILS computer system, your communications will be untraceable, undecipherable, and unidentifiable.

But you have to be smart when you're trying to stay anonymous online. You don't want to post to Facebook, as that will give away your identity and activity, even if no one knows where you are.

And you don't want to sign in to any other personal online accounts you might have — like your bank — because even though your location can't be traced, the bank's servers will have a record of your login activity.

By using TAILS and being very disciplined about his online activity — and insisting his correspondents do likewise — Snowden was able to upload documents to WikiLeaks, coordinate the timing of the leaks with Julian Assange and reporters, and arrange his flight plans out of the country.

That's an awful lot of high-visibility online activity to go undetected by any of the NSA's cyber listening posts.

Setting up and using TAILS requires technical skills that I can't impart in this e-book. If you decide you need the ultra-privacy these operating systems can give you, start Googling, or enlist the help of a

good computer person you know you can trust. Good luck!

Did I mention that TAILS is free? It's based on the open-source Linux operating system that underpins much of the internet itself. The biggest investment will be your time in climbing the steep learning curve.

And TAILS isn't the only high-privacy operating system out there. Another one, named QUBES has recently arrived on the scene, and Snowden says it looks promising.

Protecting yourself from warrantless eavesdropping isn't the only reason you might want to adopt ultra-secure computing. Corporate espionage of trade secrets and state-sponsored hacking by foreign countries are clear threats in the modern workplace. Ask the Sony executives whose careers were ruined when their insider emails were posted online for the entire world to see in 2014.

I would be remiss if I didn't warn you that security advisors say that the mere act of displaying an interest in TAILS and ultra-private computing — by Googling it or downloading it — risks you drawing the CIA's and NSA's attention. Just by writing about it to educate you, I'll probably wind up in their crosshairs.

So if you jump into the world of ultra-private computing, you must decide if the benefits of leakproof privacy and total online anonymity outweigh the drawbacks of greater scrutiny.

Our government once believed that our desire for privacy was a cherished right that must be protected. How ironic and sad that they now consider the desire for privacy an act of hostility that must be monitored!

The country's founders must be spinning in their graves. ♦

Interested in gold? Dan Rosenthal, the cranky, crusty Chief Strategist of Renegade Gold Advisory, closed out 11 recommendations last year, all winners. Average profits per reco, an amazing 144%.

For a FREE e-subscription to his Renegade Gold Advisory, email us at 3monthsfree@renegadeadvisory.com, or phone Ella at 1-866-500-6746.

Part IV

Protecting yourself from email hacks

Chapter 18

Use strong passwords for your email accounts

(Difficulty level: Easy)

How strong do you think your passwords are? How long do you think it would take a hacker to figure them out and get into your accounts?

Hackers use programs to guess your passwords and get into your accounts. These programs can guess up to millions of passwords per second — a password using only 7 numbers takes less than a second to crack.

If your idea of a good password is combining your cat's name with the two digits of your birth year at the end, I have to tell you: any decent hacker will get into your accounts within minutes — unless your cat's name is appomattoxappaloosamax.

Don't feel too bad. I took stock of my own password habits while I was writing this chapter, and I was embarrassed to discover that my passwords weren't nearly as good as I thought they were, either.

Luckily, we can do something about it. I'll show you why it's so easy for hackers to crack most passwords, but more importantly, I'll show you how to create the kinds of passwords that are really hard for hackers to crack.

I assume you've protected your router with a password, as I discussed in Chapter 13. Before I forget to mention it, you should do the same for your computer's login screen.

After you've protected your computer and routers from easy hacking it's time to secure your email accounts.

What does a strong password look like? First, let me tell you what it *doesn't* look like. Security experts tell us that the #1 worst password of all time is:

123456

That should make you laugh, but not because you recognize it as

RED ALERT

Below are a handful of the most insecure passwords ever. Do you recognize any of your passwords on this list?

Shucks, if one of your passwords is even *close* to any of these stinkeroos, you'll have about as much luck stopping a hacker as you would stopping a bullet with a balloon.

These passwords, and thousands others like them, are what hacking programs try first when they want to break into your accounts.

111111	555555
123123	654321
123321	666666
123456	7777777
1234567	987654321
12345678	google
123456789	mynoob
1234567890	password
123qwe	qwerty
1q2w3e	qwertyuiop
1q2w3e4r5t	zxcvbnm

one you use.

It should make you laugh because it's shamefully insecure. If you use that password for anything ... your computer, your router, your email login ... it's about as secure as not having a password at all!

Tragically, 123456 is the most common password people use, despite being the worst of them all.

Look, there's no excuse for being so lazy as to use 123456 as your password, or the word "password" (#2

worst on this [list of the worst passwords](#)).

That's like parking your car downtown, keys in the ignition, doors unlocked, while you head into a restaurant to meet someone for lunch — what could possibly go wrong?

Other passwords to avoid: anything that combines the name of your pet (or your spouse or children) along with someone's birth year: frodo2009 or gladys47 ... no and no.

Those passwords, and thousands like them, are baby puzzles for hackers and the automatic password-cracking programs they use. Don't be played for a sucker. Use a stronger password.

Chapter 19

How a hacker cracks your password

Let's say a hacker gets his hands on a list of stolen email addresses. There are plenty of them floating out there: Hackers have stolen the logins of 1.5 BILLION users from Yahoo alone!

Think back over past few years to all the data thefts and the billions of customer records that are now in the hands of hackers. And this is just a partial list:

- Target (70 million retail accounts)
- Sony (100 million PlayStation user accounts)
- Experian (15 million consumer credit records)
- Anthem Blue Cross (80 million health insurance customers)
- Adobe Systems (design software; 152 million user accounts)
- Ashley Madison (online site for marriage cheaters; 32 million user accounts)
- eBay (online auctions; 145 million user accounts)
- Home Depot (hardware superstore; 56 million consumer accounts)
- JP Morgan Chase (banking; 76 million user accounts)

Just stealing the logins and passwords doesn't mean your account can be taken over. First, the passwords have to be cracked.

When you login to a website online, you enter your passwords as words and numbers in plain text. But before those websites store your passwords in their databases, they first encrypt them using a standard math formula to make them unreadable. Then they store the encrypted text of your password in their database instead of the plain-text one.

It's a safety measure that prevents anyone with access to the database from simply scrolling through it and seeing what the passwords are, since all of them look like gibberish once they're encrypted with the standard math formula.

But the math formula that encrypts your plain-text password is a one-way formula: it can create encrypted text from a plain-text password, but there isn't a corresponding formula that can create a plain-text password from an encrypted one.

This is why, when you forget your password to a website, the website can never tell you what it was — they can't go backwards from the encrypted password stored in their database to the plain-text

password that you originally set up.

Instead, they can only reset your password with a temporary one and email it to you, and you have to change your password after you log in with the temporary one.

(Security tip: if a website is able to send you your original password after you've forgotten it, that tells you that the password was NOT encrypted before they stored it! And that's a big security NO-NO.)

So how does a website know the password you give when you log in is the right one, since they can't decrypt your stored password in their database and match it with your plain-text password — it's a one-way formula, remember?

Simple: the website encrypts your plain-text password with the standard math formula when you log in, then compares the resulting encrypted text with the encrypted password stored in the database under your username.

With all that one-way encryption and database matching going on, this should be a pretty safe way to keep your passwords from being revealed, right? After all, no one can re-create a plain-text password from an encrypted one!

Not so safe, after all — hackers can usually discover your original plain-text password by using the same one-way encryption and matching that those websites do. The only difference is, they feed millions of password guesses through the formula, and look for matches against passwords in the database.

This high-speed automated guessing is devastatingly effective — and the simpler your password is, the easier it is to crack.

The hacker's program generates millions of password guesses (including the old standbys 123456 and password, along with combinations of names and numbers like `aiden95` and `letmein1`).

They also test stolen passwords against databases of the most commonly-used passwords, making easy work of low-hanging fruit.

Each of the passwords generated by the program is encrypted using the standard math formula, and compared to the encrypted text

of passwords stored in the stolen database.

The program can compare thousands and thousands of passwords per second this way. And if hackers put multiple computers on the task, they can compare millions of passwords per second. A weak password doesn't stand a chance.

When the program finds a match between the encrypted text of one of its automated guesses and the stolen database — BINGO! — the hackers know what the true password is, because the program has a record of the plain-text guess that resulted in the encrypted match.

The program displays a list of user login names along with the plain-text password that matched the database. You've just been hacked!

Now that a hacker knows your original password for your email or banking account, they can log into the account and lock the rightful owner out of the account by changing the password. At that point, identity theft is a certainty.

And it gets worse for you, because most people use the same passwords on several online accounts. So when hackers crack your password, they have the keys to multiple accounts of yours.

Chapter 20

The best password is the one that takes the longest to crack

There's actually no such thing as the "best password," but some passwords are much harder to guess than others — even by a computer program capable of making a million guesses a second.

Your goal should be to make your password difficult enough to crack that a hacker will give up and move on to lower-hanging fruit — it's a better payoff for him to crack a thousand easier passwords in the database than to use CPU time on yours and have nothing to show for it after days of trying.

There are all sorts of password-creation strategies out there that claim to result in "strong" passwords that are hard to crack. Most of them end up creating weak passwords, because they strive to make it

easy for you to remember what the password is.

Such passwords will contain exploitable patterns, such as sequences of words that can be matched against a dictionary; commonly-used names or words with a number tacked onto the end; abbreviations of common phrases or prose; portmanteaux (parts of two or more words combined to form a new word); the initial letters of words from a famous quote; mathematical constants like *pi* (3.14159...), or *e* (2.71828...), or the golden ratio *phi* (1.61803...), and so on.

Passwords like these have patterns that can be statistically determined — consonants and vowels in predictable sequences and proportions, for instance.

So here's the sad, harsh truth: **If your password is easy for you to remember, it's probably trivial to crack it.**

Random combinations of letters, numbers, and punctuation offer the best resistance to automated cracking. The longer the password, the better.

But human beings are very, very bad at generating random sequences of characters. We all tend to fall into selecting characters with subtle but distinct patterns, even when we think we're being random.

You're no match for a computer. So leave the random password-picking to a computer, which is far better at "randomness" than we humans are. Later, I'll have some suggestions for apps and websites that can generate passwords for you.


First, let's see how strong your current password is. The website <http://password-checker.online-domain-tools.com/> has a useful password checker that will give you an estimate of how long it might take a hacker to crack your password.

Enter a test password in the "Password" box (note: don't click on the banner ad that looks like it has an entry box). For safety, don't enter your real password — use a facsimile that has the same basic pattern of consonants and vowels, and upper and lower case characters, but different from your real password.

You can leave as-is any numbers like years, math constants, or digits on the end that merely set your password apart from someone

Password Checker Online

Check all your site's rankings in 640+ search engines

 Rank Tracker

Password:

Strength: 85%

Evaluation: Excellent!


Password properties

Property	Value	Comment
Password length:	16	OK
Numbers:	15	USED
Letters:	0	NOT USED
Uppercase Letters:	0	NOT USED
Lowercase Letters:	0	NOT USED
Symbols	1	USED
Charset size	42	MEDIUM (0-9, symbols)
TOP 10000 password	NO	Password is NOT one of the most frequently used passwords.

Brute-force attack cracking time estimate

Machine	Time
Standard Desktop PC	About 362 billion years
Fast Desktop PC	About 90 billion years
GPU	About 36 billion years
Fast GPU	About 18 billion years
Parallel GPUs	About 2 billion years
Medium size botnet	About 362 thousand years

Dictionary attack check



'3.14159265' + '358' + '979' is not a safe word combination. The word is composed of three components: 1) The string '3.14159265' follows the pattern [dictionary word][one or two digits]. 2) The string '358' follows the pattern [dictionary word][one or two digits]. 3) The string '979' follows the pattern [dictionary word][one or two digits].

Your password is: Not safe!

The online password checker at <http://password-checker.online-domain-tools.com/> gives you a thorough estimate of how strong your password is. Even passwords that look strong — such as first 16 digits of *pi* shown here — can be cracked if they contain common numbers or words in a common order. Using *pi* as a password fails the dictionary attack check: it's "Not safe!" If you're using a password that looks strong but the dictionary attack check says it's not, scrap it.

else's (1, 2, 99, etc.). But modify any personal numbers like phone numbers, full birthdates, or addresses.

The website will gauge how strong your password is, and how long it might take a program to crack. The results might surprise you.

The biggest programmed danger facing your password comes from "botnets": a network of computers working on the same problem in sync. Botnets can have the collective power of a supercomputer.

They can crack in seconds passwords that would take a single PC years to crack.

And some passwords that might take years for a botnet to crack can be cracked in minutes by a “dictionary attack.” If your password contains common words in a common order, it is vulnerable to being cracked by a dictionary attack. Ditto for numbers in a common order.

Underneath the Brute-force time estimates on the password checker webpage is a “Dictionary attack check” that will tell you if your password is safe or not from a dictionary lookup attack. Press the “> Check!” button to get a reading (see the screenshot above).

Refresh the page (the F5 key in most browsers) in your browser for each new password you want to test.

Two general principles emerge from testing passwords:

1. The longer your password is, the longer it will take to crack it.
2. The more “random” your password is, the longer it will take to crack it.

If you combine these two principles to form a long, random-character password, it will be beyond the abilities of current mainstream cracking programs.

A password like 6&D&B9%@k!4#6A2k, for example, would take a botnet over 140 billion years to crack, AND it passes the dictionary attack check.

Time might literally run out before a password like that is cracked. Physicists predict our universe has another 5 billion years to go before it runs out of gas, and does whatever universes do when they’re spent. The time needed to crack that password is almost *30 times* longer than the time remaining in the universe. Even if physicists are off by several billion years, that won’t help much.

But never mind the hacker’s program — the chances of you or me remembering a password this complex before the end of the universe is also pretty slim. There are a couple of solutions for that.

First, let me disabuse you of scribbling your passwords on a Post-It note and sticking it on the edge of your monitor. Keeping them written down in a notebook is fine as long as the notebook is hidden away, but for heaven’s sake, don’t display your passwords the way you

stick your grocery list to your refrigerator door.

One of the truly useful solutions is using a password manager like [LastPass](#) to keep track of your hard-to-remember passwords for you. When you visit a website, LastPass will automatically fill in the username and password that you created, so you don't have to type it all out. You will only have to remember one password: The master password that unlocks LastPass. Easy enough, right?

LastPass is free, and is available on Windows and Mac as an extension for browsers like Chrome, Firefox, Safari, and Edge — and as an app for iPhones and Android phones.

Alternatively, if you like keeping track of your passwords yourself — the notebook method — you can record all your logins in a note-taking program like [Microsoft OneNote](#) (completely free, unlimited storage, syncs on multiple devices, and is built into Windows 10) or the popular [Evernote](#) (a limited amount of data storage is free, and syncing on 2 devices only; more features will cost you).

Basically, you're replacing your paper notebook with an electronic one. Both of these note-taking programs create backups online and on your hard drive, so you don't have to worry about losing them.

With the note-taking programs, you'll copy your login and password in a note, and you can look it up, and cut-and-paste from the note into the login page as needed. It's not automatic, but it's still vastly simpler than trying to remember a bunch of random passwords for different websites.

However, I have to tell you that storing your notes online doesn't guarantee they'll be completely safe from hackers. Like ANY files you store in the cloud, they could someday be hacked.

You have to decide if the convenience of anytime/anywhere access to your notes is worth the ever-present risk of hacking, and trust that the cloud storage for your notes has sufficient security to keep your files safe.

Remember to password-protect the OneNote or Evernote app on your phone. You don't want the program itself to be open-access for anyone to launch and scroll through.

Of the two programs, I prefer OneNote, because it's free, it runs on phones and PC, and Microsoft has been continually improving it.

Evernote seems to be in a contraction period — it has scaled back its features in recent months, and users have complained of declining customer support quality. Plus, their program is not free.

Also, Evernote in 2013 was the victim of a data breach that gave hackers 50 million user accounts with passwords in encrypted form. No actual accounts were reported compromised, but it left users susceptible to phishing email scams claiming to be from Evernote and directing them to a fake password reset site.

Whichever password-reminder method you choose, just promise me you won't leave your passwords scribbled on a Post-It note stuck to your computer monitor, okay?

Chapter 21

How to generate strong passwords (Difficulty level: Easy)

There are several online password generators that will create strong passwords for you. You just have to copy and paste the generated passwords into your login (and save them in LastPass or OneNote so you don't forget).

LastPass (which I discussed in the previous chapter) has a built-in password generator in their phone app and in their Chrome browser extension. You can also use their online [password generator](#).

As you know now, one of the strongest passwords you can use is a long string of random characters — alphabetic, numeric, punctuation. Make it at least 16 characters long. LastPass can create those in a snap.

You can also tell the LastPass generator to avoid certain characters (symbols, for example), or ensure a certain number of numeral characters are used. Very handy.

An alternate method to combining a bunch of random characters is to create nonsense phrases of several words that don't normally go together, like this example:

Fuschialess- Multiplicativity# Pterodactylize@ Reticentlessness&

This is a 65-character password consisting of all four words. Normally, word-based passwords can fall to a dictionary attack if you

use only two or three common words.

But each of the words I've used are unlikely to be found in any dictionary, much less all four of them. To further confound a dictionary attack, I've added suffixes that are grammatically almost correct, even if they aren't meaningful.

A long enough password like this one (four or five words, totalling 30 characters or more) is much harder for a dictionary attack to crack — especially if you mix upper-and-lower case letters, and embed punctuation or number characters in them as I've done above.

Password-checker.online-domain-tools.com estimates that my 65-character password of words would take a botnet “About 5 trestrigintillion years” to crack. That's an actual magnitude, and I have no idea how many zeros that is. But I'll bet it's a lot.

Some websites will let you use spaces in your passwords, others won't, so you might have to experiment with how your password has to be formatted. Also, some websites might insist that your password contain at least one number, so you'll have to take that into consideration too.

Some websites might limit how long your password can be, and you might not be able to use a long password. I weep when I see this, because it's a programming decision so absurd that it could only have sprung forth from the mind of an incompetent programmer.

Here's why: the standard math formula that I told you about in Chapter 19 — the one that encrypts your plain-text passwords before storing them in the database — creates encrypted texts that are always 60 characters long, no matter how long the plain-text password is. It sounds bizarre, but it works.

Feed the formula a 6-character plain-text password, and you'll get back encrypted text that is 60 characters long. Feed it a 500-character plain-text password, and you'll get back encrypted text that is 60 characters long.

Get it? No matter how long the plain-text password is, the formula will consistently create a 60-character-long encrypted text from it. *The length of the plain-text password is irrelevant.* The encrypted passwords stored in the database are always going to be 60 characters long. That's why putting a limit on the length of a login

password is asinine.

In terms of a password strategy, I think you have a better chance of remembering four or five nonsense words with punctuation around them, than sixteen random characters. So pick your phrase carefully, test out a facsimile on the password checker, and let a password cracking program choke on your password the next time your login info gets stolen in a massive data breach.

A related strategy is to use a lengthy phrase from a story or poem that you can remember. Properly capitalize and punctuate the phrase to give it variety: an example would be the first stanza of Jabberwocky. But since this is a well-known poem, you'll have to use a lengthy snippet of prose to defeat the dictionary attack.

The first two lines of Jabberwocky yield a botnet cracking time of 462 trestrigintillion years — almost a hundred times better than my four nonsense words! It's the longer length that gives this password extra strength.

Another strategy worth mentioning involves extracting the first or second letter from the beginning of each word of a memorable-to-you sentence. You can create some moderately tough-to-crack passwords that are easy for you to remember this way.

Do you think you'd have a hard time remembering a password like 4SA7YA0FBFUTC ? It's the first letter of each word from the opening of The Gettysburg Address.

Because passwords of this type have a limited pattern of characters to pick from, a botnet could crack it in about 20 days. So while it's not the weakest password you could choose, it's not as good as 462 trestrigintillion years, either.

This style of password has the benefit of being fairly easy to remember, at the tradeoff of being easier to crack than some of the other password types we've discussed.

Maybe on some recreational or news websites where you don't store any personal information, and you don't care if the password is weaker than what you use for online banking, this type of password would appeal to you.

But for your high-value logins, use as strong a password as you can.

Chapter 22

More password dos and don'ts

- ▶ **Don't** share your passwords with anyone unless you have to
- ▶ **Don't** use the same password on multiple websites. If a hacker gets your password to one site, he has it for a bunch of websites, and can gather more identifying information about you from each one
- ▶ **Don't** use passwords that are the same except for one character or a number at the end. If you're going to make them a tiny bit different, you might as well go a step further and make them a lot different
- ▶ **Do or don't** change your passwords every year or so. There's a split opinion on this one. Some experts say changing your passwords at least annually is good, because it's more difficult for hackers to crack a moving target.

Other experts say changing your password tips off hackers that your account is active, and worth the extra effort to crack. These experts advise picking a strong password and letting it stand.

I don't care whether you change passwords annually or not, as long as you're using a strong password. Some websites force you to change your password periodically anyway, so you might not have a choice in the matter.

Chapter 23

Answering the so-called "Security Question": Lie!

Some websites, when you first sign up for them, require you to answer a few "security questions" that they can use to confirm your identity along with your username and password.

The questions are often common facts about you, such as:

- ☒ What was the name of the last high school you attended?
- ☒ What is your mother's maiden name?

- ✓ In what city were you born?
 - ✓ How many siblings do you have?
 - ✓ What is your father's middle name?
 - ✓ What was the name of your first pet?
 - ✓ What are the last two digits of your birth year?
 - ✓ What color are your eyes?
- ... and so on.

Besides being incredibly intrusive, these questions are ANTI-security. If a hacker stole the answers to such questions from a website, and combined it with other information they can glean about you, they would be able to construct a pretty complete profile of you to aid in their efforts to steal your identity.

So if you're confronted with these "security questions," don't answer them truthfully. Lie!

What is your father's middle name? "Mxyzptlk." In what city were you born? "Valhalla." What was the name of the last high school you attended? "The School of Rock." What color are your eyes? "Rainbow."

You get the idea.

Chapter 24

You have to tell Outlook, Thunderbird, or Entourage to encrypt your email ... otherwise it's sent openly like a postcard (Difficulty level: Medium)



Some technical terms ahead.

If you log in to Gmail or Yahoo email on a browser, you can skip ahead to Chapter 25.

You can also skip this section if you use Exchange Server.

But if you use a program such as Outlook, Thunderbird, or Entourage to manage your email, this section is important.

Many people prefer using email programs like Outlook,

Thunderbird, and Entourage instead of webmail. The big reason is that the email programs let you save your email messages on your computer permanently, instead of in the cloud, where they are subject to the whims of your internet connection or cable company. You can refer to the saved emails even when you're offline.

Using an email program like Outlook can also be safer than webmail. Outlook and the other programs can download your emails from the email server to your hard drive and then delete them from the email server. This way, even if a hacker gets your email password, he can't download all your prior messages from the email server, because they are gone from there — but safely stored on your hard drive.

Also, email programs like Outlook let you collect messages from more than one email account at the same time, and view them all in a single Inbox. Much easier to organize that way. With webmail, you have to log in to each account separately, and switch between tabs to view them.

And finally, using an email program like Outlook, instead of reading your emails online in a browser, eliminates the ads that appear alongside your emails with some email services like Yahoo.com.

Whatever method you use to handle your emails, once an email leaves your computer, it gets handed off through a network of computer servers called *mail relays*, which are like post offices, except electronic.

When you send a letter from Oregon to Florida using snail-mail (the USPS), it might pass through several regional post offices along the way before it winds up at the recipient's local post office for delivery.

Likewise, email messages can zig-zag their way from the sender's computer through a network of mail relays before finally reaching the recipient's Inbox.

These mail relays have the ability to send email messages across the internet with encryption, or without it. Encrypted email is like sending a letter sealed inside an opaque envelope; unencrypted email is like sending a postcard. The sender's email program has to tell the server which method to use.

When you set up an email account in a program like Outlook, it automatically fills in some basic email server settings so you can send

and receive messages. But the basic settings in Outlook default to sending and receiving unencrypted email.

Unencrypted email is self-explanatory. If a hacker were to intercept your emails by tapping into the network that connects your computer to the email server, he would be able to read all of your inbound and outbound emails without any problem.

But you can tweak a couple of settings in Outlook and make it encrypt all the messages it sends and receives, making your emails more hacker-proof. This works with most email services, including Gmail, Yahoo, and Outlook.com.

By default, Outlook chooses the insecure method for sending and receiving emails when you add an email account, because it's simpler for them and for you. But you have to override that and tell Outlook to use the secure email settings.

The encrypted email protocol — called TLS/SSL (TLS is newer; SSL is older and will be phased out) — uses the same encryption technique as <https://>, which you'll see in front of a website address when you purchase something from an online store, or view your banking balance online. HTTPS tells your computer to encrypt everything that happens on that web page before sending it out over the internet, so your private transactions stay private.

So it is with TLS/SSL email. If you tell Outlook to encrypt your email with TLS/SSL, and a hacker intercepted them, it wouldn't do him much good. All he'd see is a bunch of gibberish.

You can make Outlook (or other program) use secure TLS/SSL encryption when it sends and receives email, but you'll need to supply it with some settings that only your email provider can give you.

You can likely find the settings your program needs by searching Google for “server settings for [email provider] with [program and version]” (e.g., “server settings for everyone.net with Outlook 2013”).

**NOTE**

The details you need to use TLS/SSL in Outlook, Thunderbird, or Entourage are unavoidably technical. The steps are different for every program, every version, and for every email provider. Contact your email provider's tech support for assistance if needed.

Chapter 25

Types of email accounts and what Outlook needs to use them

You can skip this chapter if you don't use Outlook, or if your Outlook is already set up for your email account.

The general instructions provided in each category below may not apply to you. If you're not sure which category applies to you, or how to find instructions to set up an email account, ask a computer support person for assistance.

Your email account falls into one of three categories:

1. **Free email accounts.** The big guns in free email are Gmail.com (by Google) and Outlook.com (by Microsoft). Those two free email services offer huge storage space, and integration with many other useful online tools like calendars, free cloud storage, and AI assistants that can remind you of an upcoming bill that arrived in your Inbox.

Yahoo.com is another popular choice for basic, personal email, but it doesn't have the useful addons that Gmail and Outlook.com do. And I would discourage you from using it.

Why don't I like Yahoo? Because Yahoo has proven itself to be very lax when it comes to security. Their CEO, Marissa Mayer, ignored warnings from her cyber-security group that the company needed to boost its security structure.

The result: over 1.5 billion user accounts were stolen from Yahoo in the largest cyber-hack in history.

Other free email options include iCloud.com (Apple), aol.com (AOL Time Warner), and Zoho.com.

With the popular free email services, programs like Outlook can automatically fill in a lot of the account information itself when you add your email address to the program.

If you use a free email service, search Google for instructions on how to set up your version of Outlook (or other program) for it.

2. **Custom email account through a private email hosting provider.** If you have a custom email address with your own .com domain, it's likely through a private email hosting provider. Maybe your work set it up. Maybe you bought a website domain that has email accounts with it.

Custom email accounts aren't free, so you'll usually pay a monthly or annual subscription fee to have them. An example of a custom email address from a private hosting provider would be `tom@floppyochre.com`.

Outlook's setup wizard can't automatically fill in the settings for a private email account like it can for popular free accounts, so you'll have to ditch the setup wizard and do a manual setup, supplying Outlook with some technical information like server names and port numbers for your email address.

You can likely find the settings your program needs by searching Google for "server settings for [email provider] with [program and version]."

Example: Let's say my `tom@floppyochre.com` custom email address is hosted by Everyone.net, and I want to use Outlook 2010 to send and receive emails. I'll search for "how to set up Outlook 2010 with Everyone.net email", and follow the instructions given by one of the search results.

I'll be sure to select TLS/SSL encryption in the fields that ask for it (see a later chapter for more on this).

3. **Cable provider email accounts.** These accounts come included with your monthly cable service. If your email address ends in `comcast.net`, `rr.com`, `charter.net`, `att.net`, `bellsouth.net`, `verizon.net`, `cox.net` or others like it, you have a cable provider email account.

Cable provider email accounts might seem handy because you get them along with your cable subscription. It's almost like they're free.

But they have a number of drawbacks that make them less than ideal for your primary email, and I'll cover those in a later chapter.

A better choice for email is Gmail, or a custom email account.

Chapter 26

POP3 or IMAP?

POP3 and IMAP are two different methods of handling email between the email server and you. Outlook (or other program) will ask you to choose which type of mail handling you want to use when you set up an email account.

- ▶ Use **POP3** if you only use your email address on one device, such as your PC.
- ▶ Use **IMAP** if you want to use your email address on multiple devices like your computer, phone, and tablet.

IMAP will automatically synchronize the emails on your phone and computer when they're logged into the same email account. (More on IMAP in a later chapter.)

Chapter 27

Port settings and TLS/SSL



Some technical terms ahead.

When you set up an email account in Outlook or other program, it needs to know what port numbers to use for sending and receiving email. The email port numbers available to your program are determined by your email provider.

They can be a confusing part of the set up in any email program, because there are usually several to choose from.

I'll try and simplify that for you.

In general, the following port numbers do not use TLS/SSL encryption, so your emails will be sent insecurely (Outlook will use these as the default if you don't override them).

If your email account has been set up with these settings, do a Google search to find out what settings you need to use for TLS/SSL with your email provider. The port numbers to avoid are ...

For incoming mail, POP3 on port **110**: INSECURE.

For incoming mail, IMAP on port **143**: INSECURE.

For outgoing mail, SMTP on port **25**: INSECURE.

For outgoing mail, SMTP on port **26**: INSECURE.

For outgoing mail, SMTP on port **2525**: INSECURE.

For outgoing mail, SMTP on port **587**: INSECURE.

For secure email with TLS/SSL encryption, override the use the following port numbers when you set up your email account in Outlook or other program:

For incoming mail, POP3 protocol on port **995**: SECURE.

For incoming mail, IMAP protocol on port **993**: SECURE.

For outgoing mail, SMTP protocol on port **465**: SECURE.

Be sure to select TLS/SSL encryption where it is listed (Google it to find out where that is for your program).

You can also use Google to search for how to set up your mobile devices like iPhones, Android phones, and tablets with TLS/SSL email encryption. There, you'll be using apps instead of programs, but in general, the same account settings that Outlook needs, your phone needs also.

Chapter 28

Why you should avoid cable provider email accounts

If you have cable TV service in your home, you probably get your internet through them, too. And I'll bet you got a free email address along with it.

As I mentioned previously, email addresses that end in comcast.net, rr.com, charter.net, att.net, bellsouth.net, verizon.net, cox.net or others like it, are cable provider email accounts.

Free email with your internet service — what's wrong with that? Plenty!

- If you change cable companies because you move, or because you sign up for a better deal with a different cable company, guess what happens to your old email account? It gets deleted, because you're no longer a customer! All your emails, gone. No chance of

recovery.

However, if you use an email address from Gmail or Outlook.com, it will stay yours forever — no matter how many times you change cable companies, and no matter where you move to. Your emails can't be held hostage by a cable company, because they don't own the account.

- Do you want to use the same email address on your phone and PC? Lots of people do. But many cable company email accounts only use the POP3 email protocol, which does not sync emails between devices.

That means if you clean out a bunch of old emails on your phone, you have to go over to your PC and delete them there, too. What a hassle!

By contrast, Gmail and Outlook.com support the IMAP email protocol, which is perfect if you want to use the same email address on your phone and PC. With IMAP, whatever you do with email on one device is automatically mirrored on the other.

Send an email from your phone, and it automatically shows up in the Sent Items folder on your PC. Delete an email on your PC, it automatically gets deleted from your phone.

- Cable company email services often don't give you the option of using TLS/SSL email encryption to keep your messages hacker-proof. They only let use the insecure protocol to send and receive your emails.
- You might not be able to use your cable provider email account on your phone, outside your cable provider's service area.

With a Gmail or Outlook.com email address, you can just as easily send emails from Taipei as you can from home.

Chapter 29

Use “two-factor authentication” for your online email accounts if you’re a privacy fanatic (Difficulty level: Easy to Medium)

If John Podesta, Hillary’s campaign chair, had enabled two-factor authentication in his Gmail account, hackers would not have been able to steal his emails — even though they had his password, which he unknowingly gave them.

With two-factor authentication turned on, Gmail would have sent a confirmation code to Podesta’s phone, which the hackers didn’t have.

Without the confirmation code to complete the login, Gmail wouldn’t have allowed the hackers into Podesta’s Inbox. Podesta would have been alerted that hackers were trying to get into his email when the confirmation code appeared on his phone unexpectedly.

The hackers would have been denied. 50,000 of Podesta’s emails would be safe and sound in his Gmail account. Donald Trump would be back running his golf courses and hotels. And President Hillary would be fighting with the Republican-controlled Congress over Muslim immigration policies.

Two-factor authentication is basically a two-step login. In addition to your password, there’s a code number you have to confirm.

The code number changes each time you log in, and it arrives as a text message on your phone. You have to type the code number on your login page as verification that it’s really you logging in.

The security idea behind it is that it’s far less likely that a hacker will have stolen your password AND your phone at the same time, so they will not be able to confirm a confirmation number sent to your phone.

Right now, two-factor authentication is only available with a handful of email accounts: Gmail, Outlook.com, Yahoo, AOL, and a few others.

(For a list of email services and other online logins that allow two-

factor authentication, see <https://twofactorauth.org/#email>.)

Two-factor authentication currently works only on browsers, or apps that are built to accept both a password and a code number during login.

Standalone email programs like Outlook, Thunderbird, or Entourage can't handle it because they can only send a password, not a password plus a confirmation code from your phone.

But since so many people use programs like Outlook to manage their emails, Google has developed a "cheat" that allows these programs to log in even though they can't perform the second part of the two-factor authentication login.

Google created a special password for you to add to Outlook and other programs *in place of your regular email password*. When Outlook logs into Gmail with the special password, Gmail skips the second part of the two-factor authentication and lets Outlook fetch your emails as normal.

You, on the other hand, will still use your regular password when you log into Gmail from a browser, and you'll have to verify the confirmation code for security. The special password is just to let Outlook continue working, even when two-factor authentication is turned on in Gmail.

Interested in gold? Dan Rosenthal, the cranky, crusty Chief Strategist of Renegade Gold Advisory, closed out 11 gold stock recommendations last year, all winners. Average profits per reco, an amazing 144%.

For a FREE subscription to his Renegade Gold Advisory, email us at 3monthsfree@renegadeadvisory.com, or phone Ella at 1-866-500-6746.

Chapter 30

The email hack that scuttled Hillary's presidential hopes — and how you can avoid falling for the same scam

It was the simplest of email scams, yet it felled a presidency. It could have easily been recognized and avoided, but it wasn't. In this section I'll show you how you can avoid getting taken for a sucker like Hillary's campaign did.

Most people think of email scams as laughable hoaxes like the Nigerian prince who asks if you would allow them to deposit millions of dollars into your bank account for safekeeping, for which you will be guaranteed a handsome reward. To get the process started, you just need to send your banking account information to the prince's representative, and pay a modest few thousand dollars in paperwork fees and taxes, but it will all be reimbursed many times over.

Surprisingly, people fall for that hoax and wind up sending tens of thousands of dollars to the scammers, never to see the money again. Most of the victims are elderly, and shockingly oblivious to being hoodwinked.

Then there was the famous hoax email from "Bill Gates" that asked you to forward the message to a bunch of your friends as part of a Microsoft email tracking experiment. When the email reached 1,000 people, each of them — including you — would receive \$1,000 from Bill Gates himself!

A few of my computer-illiterate friends fell for the Bill Gates hoax when it first appeared, but fortunately that hoax was harmless. Of course, they received nothing for their efforts, except maybe mild embarrassment for being so gullible.

Today, though, hackers and scammers have upped their game. Hoaxes are no longer laughable narratives brimming with poor spelling, awkward grammar, and a complete lack of credibility.

Today's hoaxes are often sophisticated, subtle, and highly credible. They have a new name, too: **phishing**.

Phishing differs from the traditional online hoax in that rather than trying to extract thousands of dollars from you directly, phishing emails attempt to trick you into giving up your login and password information for an email account or a bank account, under the ironic pretense of securing your account from a data breach.

Armed with the login and password, the hackers can drain your bank account, ring up massive charges on your credit card, or maybe torpedo your presidential campaign.

Some phishing emails purport to be from the IRS, and ask you to enter your Social Security Number as part of the login. Using your SSN, hackers can open up new credit accounts in your name without your knowledge, and destroy your credit rating. They can make it very nearly impossible for you to qualify for a loan for a home or a car.

Many phishing emails look legitimate, because the layout will be carefully designed to match real emails the company would actually send. If hackers are phishing for bank accounts, their emails will contain the bank's logo, disclaimer statement, typographic style, marketing tagline — even much of the body text — copied and pasted directly from a legitimate email message from the bank.

Usually, the email ominously states that an attempt to gain unauthorized access was detected on your account, and for your security, you need to reset your password immediately. And the email helpfully provides you with a link to an online form where you make the change after you enter your current login and password information.

The trouble is, the link to the password-change page goes to the hacker's website, not the company's. But it looks like the company's website, right down to the typography and logo. It's clever enough to fool most people, and they follow the directions to enter their current login and password prior to choosing a new password for their account. Their login and password is now in the hands of hackers, and the real fun begins — for them.

So what do you do if you receive a message warning you that your bank account, or email account, or credit card account, had an unauthorized login attempt? Do you ignore it?

If it asks you to click a link or button to change your password,

then YES, IGNORE IT. Remember this easy-to-follow rule:

NEVER, EVER click on a link inside of an email that mentions anything about changing your account login or password.

Stop, think. But don't click the link.

It might look like a convenient shortcut to just click on a button that says “CHANGE PASSWORD” or click a link that says “Change your password now” or “Follow this link to change your password” — but if you do, you'll be sorry.

The only way you should change your password is the safe way:

Log in to the home page of your bank or email account as you normally would (e.g., wells Fargo.com, gmail.com, outlook.com, chase.com, etc.).

Find your account settings. It might be in a menu. It might be in an icon. It might be called “profile” or “preferences” or “settings” instead of “account.” No matter. Every bank website and email website has a link to your personal settings, including the password.

In Gmail, it's under the icon at the upper right. On most banks, it's in a menu, and might be called My Settings or My Profile or My Account, or something like that.

From the bank's home page you can search for “change password” and follow the instructions in the relevant result page.

This is safe, because all of the instructions are originating from the bank's website itself, and not from within an email.

If John Podesta had gone to gmail.com and just clicked on his account icon instead of clicking a link in the email, he could have changed his email password safely and quickly. And Hillary would probably be sitting in the White House today.

Ironically, Podesta wasn't a total dope. He was rightly suspicious of the email that urged him to change his password. But he didn't know what to look for to decide for himself if the email was legit or fake, and so he left it up to someone else — supposedly more knowledgeable — to decide for him. But that person turned out to be the dope.

The impact was catastrophic: 50,000 emails from his Gmail account poured into a hacker's Inbox and ended up on WikiLeaks.

Chapter 31

Is that email really a phishing scam? What to look for (Difficulty level: Easy to Medium)

A simple rule that will save you 99.9% of your headaches:

If you're not sure, **don't**.

Below are a few clues that should make you suspect a phishing scam. By itself, one of these clues doesn't always mean you're being phished. But two or more clues in a single email raise the stakes considerably.

- They contain links to obscure website addresses like bit.ly, goo.gl, tinyurl.com, ow.ly, is.gd, buff.ly, adf.ly, bit.do, x.co, mc.af. ee. The presence of a link like this is always suspect, but you'll need to look for other clues before you can say for sure it's a phishing scam. (I'll explain below how to safely find out where that short link actually lands.)
- Check the FROM address. If the from address comes from you, and you didn't send a message to yourself, it's a phishing email.
- The email has no personal salutation, and you don't know who the sender is. Message may simply begin, "Hey," or "Hi, there!" or a similar chummy greeting. This clue, along with one or more of the other clues, means it's a phishing email.
- The email salutation isn't your name, it's your email address, as in, "Dear tom7731@yahoo.com." Sometimes, legitimate emails use your email address as your salutation, but not often — it's hokey and low-tech. If you don't recognize who the sender is, it's probably a phishing email.
- It's probably a phishing email if it has an attachment that you weren't expecting to receive. DO NOT OPEN the attachment, because it's probably malware that will let a hacker take over your

computer, empty your bank accounts, and max out your credit cards.

Other clues that point to your email being a phishing scam include:

- It comes from a sender you don't know
- The subject has a generic subject referring to:
 - ✓ An invoice ("Please confirm your order total")
 - ✓ A billing statement ("Monthly statement for your approval")
 - ✓ A bank statement ("Your account has been suspended due to suspicious transactions")
 - ✓ Medical bills ("Your co-pay balance is now past due")
 - ✓ An item on backorder ("Your recent purchase has been backordered")
 - ✓ A disputed bill ("Payment declined for order A2344-56910688 — immediate attention required")
 - ✓ Automated notice from FedEx Home Delivery ("This is FedEx. We tried to deliver your package, but no one answered the door. [Click here](#) to schedule a new delivery.")

The subject lines above all seem very credible, and might even coincide exactly with something you recently did. That's precisely why they're so dangerous, and so many people fall for them.

- Any message that claims previous attempts to contact you have been unsuccessful, and your immediate response is needed, but ...
 - There is a link for you to click
 - There is an attachment for you to open

When in doubt, don't click the link. Don't open the attachment. Just delete the email.

If the email is legitimate, and your action is truly required, the person sending it will attempt to reach out to you again and will be more specific about it.

Or, visit the home page of the email's supposed sender, and review your orders, your balance, or change your password. But do it from the website you know, not the website given to you in an email.

```
> Hi John
>
> Someone just used your password to try to sign in to your Google Account
> john.podesta@gmail.com.
>
> Details:
> Saturday, 19 March, 8:34:30 UTC
> IP Address: 134.249.139.239
> Location: Ukraine
>
> Google stopped this sign-in attempt. You should change your password
> immediately.
>
> CHANGE PASSWORD <https://bit.ly/lPibSU0>
>
> Best,
> The Gmail Team
> You received this mandatory email service announcement to update you about
> important changes to your Google product or account.
```

Screenshot of John Podesta's phishing email. Can you spot the phishing clue?

Chapter 32

How to spot what John Podesta and Hillary's IT team missed

Podesta and Hillary's IT team didn't see the hack coming that was right in front of their eyes. The ugly comedy of errors that led to John Podesta's email account getting hacked is [explained in detail here](#).

What the article got wrong is that Hillary's IT team did NOT correctly identify the original email supposedly coming from Google as a fake. They thought it was legitimate. They, too, were taken in by the verisimilitude of the phishing email because they weren't paying close enough attention.

Had they spotted it, the IT team would have told Podesta, "The email that is supposedly from Google is fake. It is a phishing scam to steal your password. DO NOT CLICK ON THE LINK. Delete the email, then log into your Gmail account as you normally do. Go to your Google Account Settings (click the icon in the upper right of the email screen) and change your password there."

By itself the phishing email does appear benign, even legitimate. It addresses Podesta by his first name and not by his email address. It doesn't have any obvious spelling errors in it. It appears to offer helpful information for his account.

There are two troubling clues that this is a phishing email.

The first is that the email is asking Podesta to click on a link to change his password, rather than telling him to visit his account page at Gmail.com and change it from there.

The second is the odd link <https://bit.ly/1PibSU0>.

The problem is, you have no idea where an odd link like that will end up taking you. It's an abbreviated link that hides its true landing page. You don't want to click on the link directly, since it might download malware or trick you into coughing up your login password.

But it's easy enough to find out what the actual website address is, safely — and Podesta's IT staff should have done that.

On the next few pages are the four crucial steps that Hillary's campaign team missed, that spelled the difference between President Hillary and President Trump.

Use the Chrome browser to complete these steps.



NOTE

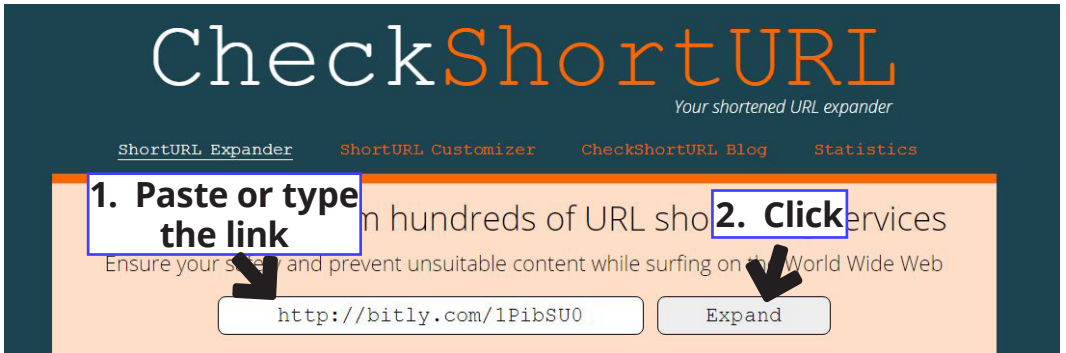
If you're tech-savvy, you can complete these steps yourself. If you're not, I suggest you turn this over to a friend or employee who can handle the technical steps for you.

You suspect a phishing email has landed in your Inbox. It looks like it *could* be legitimate, but there's a link in it that makes you think it could be a scam. How can you tell for sure?

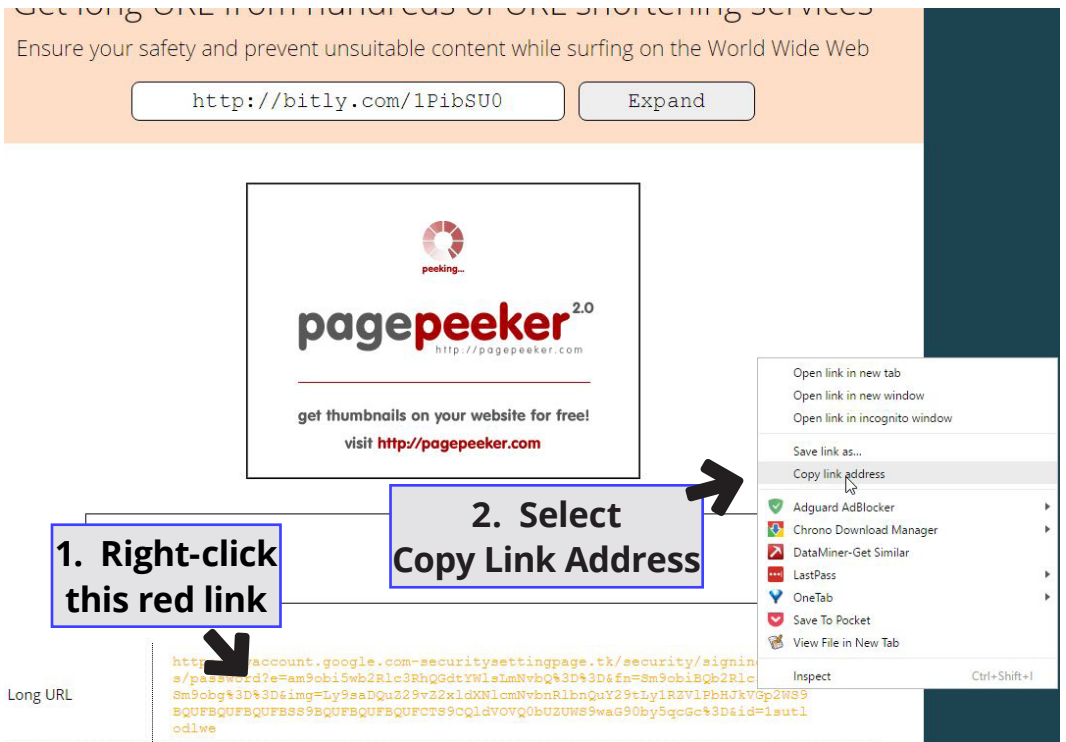
Locate the link in the email that you're supposed to click. In the Podesta email, the suspicious link is <https://bit.ly/1PibSU0>.

We'll use Podesta's email for our learning example. Of course, this is just one example. The suspicious link will be different in each phishing email you receive. Use your mouse to copy the link for further testing.

1. Go to <http://checkshorturl.com/expand.php> and paste the suspicious link into the box at the top, then click the Expand button.



2. The actual address (Long URL) that the suspect link directs to, will appear in red below the ads, labeled **Long URL**. Right-click that long red address and select *Copy Address Link* in Chrome. (The long link, like the short one, will be different for every phishing email.)



- Go to <http://www.freeformatter.com/url-parser-query-string-splitter.html> and paste into the box labeled “Copy-paste your URL here”. Click the PARSE button.

This website will split that long URL into separate pieces to make it easier to spot the phony landing page. Ignore the encrypted gibberish text, as we can’t get much information from it.

Look at the field labeled Domain. It should match the purported sender of the email: google.com, wells Fargo.com, fedex.com, etc. Does this look like a Google or Gmail web address to you? Hell, no! The domain says **com-securitysettingpage.tk**. SCAM!

To learn more about the structure of a URL, check out the [URLs Explained](#) section of this page.



The screenshot shows the URL parser interface. A text box contains the URL: `http://myaccount.google.com-securitysettingpage.tk/security/signinoptions/password?e=am9obi5wb2Rlc3RhQGdtYWlsLmNvbQ%3D%3D&fn=Sm9obiBQb2Rlc3RhOGQ%3D%3D&img=Ly9saDQuZ29vZ2xldXNlcmNvbnRlbnQuY29tLy1RZVlPbl`. A blue button labeled "PARSE" is below the text box. Two annotations are present: a pink box with the text "1. Paste the link" and an arrow pointing to the text box, and another pink box with the text "2. Click" and an arrow pointing to the "PARSE" button.

URL Parts

Scheme:	http
Protocol:	http
Authority:	myaccount.google.com-securitysettingpage.tk
Host:	myaccount.google.com-securitysettingpage.tk
Host:	myaccount.google.com-securitysettingpage.tk
Subdomain:	myaccount.google.com-securitysettingpage.tk
Domain:	com-securitysettingpage.tk
Tld:	tk
Resource:	/security/signinoptions/password?e=am9obi5wb2Rlc3RhQGdtYWlsLmNvbQ%3D%3D&fn=Sm9obiBQb2Rlc3RhOGQ%3D%3D&img=Ly9saDQuZ29vZ2xldXNlcmNvbnRlbnQuY29tLy1RZVlPbl

3. Does the domain name make sense?

At this point, you’ve identified the phony link, so technically your job is done. But if you want to peel back one last layer of the puzzle, highlight that domain name with your mouse and copy it, and move on to the next step.

4. Go to <http://www.domainhistory.net/> and paste the domain name into the search box. Click the Search button.

This final website check tells you that the domain name `com-securitysettingpage.tk` is currently inactive, because there is no registration info associated with it, just a list of blank owner records indicating it changed hands over a dozen times. *However, last year, someone owned the domain name, and you can bet it wasn't Google.*

When a suspect link points to a domain name that doesn't match the name of the company it's supposed to be from, it's a phishing scam.

You know what to do: delete that email.

There you have it. You just became a better email phishing sleuth than Hillary's campaign manager and her entire IT team. Congratulations!

Refer to these tips the next time a suspicious email lands in your Inbox, and you'll never be the sad victim of a hacker's phishing scam — like Hillary was.

Chapter 33

Stay protected and up-to-date as new threats emerge

The techniques in this book will work today, and probably continue working quite well tomorrow and into the near future.

But we can make no guarantees when we have arrayed against us the CIA, NSA, Iranian government hackers, Russian government hackers, Chinese government hackers, and Israeli hackers trying to crack the security measures we laid forth in this book.

We're sorry, but these people are good — just because they're doing bad things, doesn't mean they're not extraordinarily skilled. We'd be amazed if they didn't crack some of our solutions before long.

And we'll be working to find new ways to plug their cracks. Computer privacy is really a cat-and-mouse game. You and I are the

mice, but as Snowden and Assange have shown us, sometimes the mice can roar.

To stay updated, give us your email address, and we'll send you FREE future editions of this e-book.

Email us at freeupdates@renegadeadvisory.com, or phone Ella at 1-866-500-6746.

Dan Rosenthal, Editor
Renegade Gold Advisory

Tom Lundin, Senior Technology Analyst
Renegade Gold Advisory

Renegade Gold Advisory
318 North Carson Street #208
Carson City, NV 89701

About the authors



Tom Lundin is the Senior Technology Analyst at *Renegade Gold Advisory*. A self-taught computer programmer, his background spans four decades across a range of fields including production management, graphic design, IT management, software development, data analysis, copywriting, and online content generation.

Recently, he was a consultant and troubleshooter for an overseas call center, providing advice on setting up database operations, email marketing, and phone systems.

Tom's duties at Renegade Gold Advisory include IT, data analysis, programming, copywriting, and design, to make operations and marketing more effective and high-impact.



Dan Rosenthal saw early-on the importance of Hillary's flub on email, and said, "Trump will pull off the upset of the century and sweep into the White House."

Dan, the cranky, crusty Chief Strategist of Renegade Gold Advisory, has 6 decades' experience making money in gold and silver. As a 10-year old kid, he made a \$41 investment in silver and parlayed it into \$7,000, to help pay his tuition at MIT.

He parlayed a \$26,000 gold stock investment into \$1 million in the 1990s. In 2003, with gold at \$300, he turned bullish, rode gold up to \$1,600, and turned bearish.

Last year, in a sloppy gold market, Rosenthal closed out 11 recommendations, all winners. The profits per recommendation averaged an amazing 144.9%. This year, after just two months, his average open recommendation, two losers included, is already up more than 60%.

To receive a FREE 3-month e-subscription to his Renegade Gold Advisory, email us at 3monthsfree@renegadeadvisors.com, or phone Ella toll free at 1-866-500-6746.



RENEGADE GOLD ADVISORY
Stop losing money in gold and start making it