

**THE**

# **INVISIBLE PATRIOT**

**2015 EDITION**



How to Take Back Your Right  
to Privacy from Snoops

## Table of Contents

<b><u>1. THE ARMOR PLATED COMPUTER: HOW ENSURE THAT YOUR HARDWARE, SOFTWARE, AND PERIMETER DEFENSES ARE SECURE</u></b>	<b>3</b>
USE A SECURE BROWSER	3
GOOGLE CHROME	4
MOZILLA FIREFOX	6
BEST FREE ANTI-VIRUS SOFTWARE	8
AVG FREE	8
AVAST	9
WHAT IS SPYWARE?	10
SUPERANTI SPYWARE FREE EDITION	11
YOUR COMPUTER MAY BE INFECTED IF...	12
SECURE YOUR WI-FI CONNECTION	13
PUBLIC WI-FI SECURITY	14
<b><u>2. HOW TO CREATE UNHACKABLE PASSWORDS</u></b>	<b>15</b>
PASSWORD DOS AND DON'TS	16
<b><u>3. PROTECT YOUR INBOX</u></b>	<b>21</b>
SECURE EMAIL TIPS	23
SECRET AGENT EMAIL TACTICS	24
OPENING EMAIL ATTACHMENTS	25
<b><u>4. SECURE ONLINE BANKING AND SHOPPING</u></b>	<b>27</b>
ON YOUR END...	27
SECURE SHOPPING TIPS	28
VIRTUAL CREDIT CARD NUMBERS	29
SECRET AGENT TRICK	30
<b><u>5. SHIELDING YOUR OFFLINE PRIVACY</u></b>	<b>32</b>
MONITORING YOUR IDENTITY	32
FREEZE YOUR CREDIT	33
POSTAL AND DELIVERY SECURITY	34
ANOTHER MAIL TRICK	35
SUBPOENA THE IRS	35

# **1. The Armor Plated Computer: How Ensure That Your Hardware, Software, and Perimeter Defenses are Secure**

## **Use a Secure Browser**

Once upon a time, the majority of the software and media on your computer was installed through disks, DVDs, and CD ROMs. Now, almost 99.9% of the information stored on your computer is downloaded directly from sources on the Internet. There are ways to verify the authenticity of all of these downloads, but you must have a security plan in place in order to filter out the viruses, malware, and scams.

Since the Internet is the source of almost all of the software, your security plan must start with selecting a secure web browser. The Internet browser you choose is your first line of defense, so choose wisely.

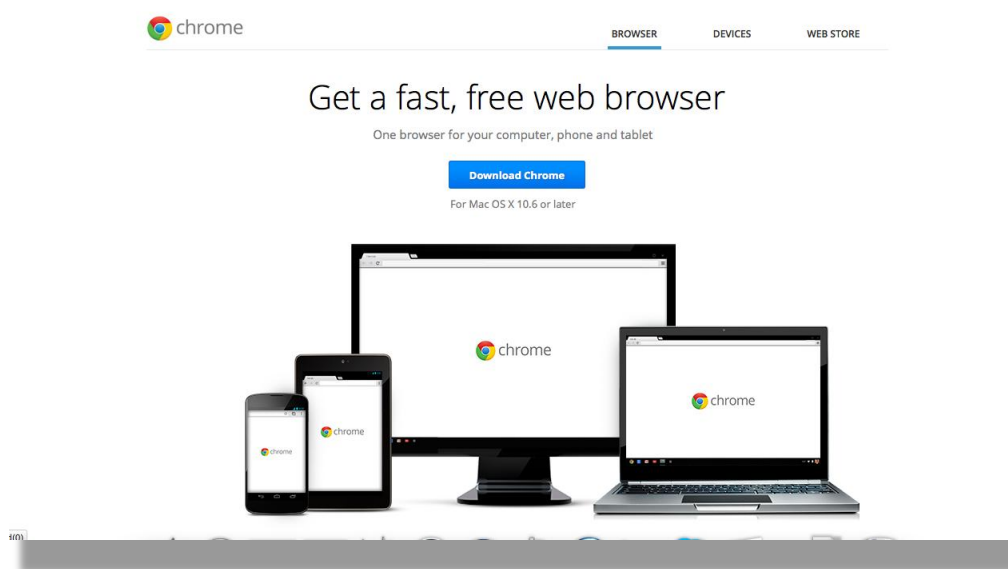
Internet Explorer is by far the most commonly used browser on the planet, which is why most hackers focus on developing viruses to exploit any weak spots in Internet Explorer's defenses. Thus, through no fault of Microsoft, its users are targeted at a higher rate. Simply choosing a less popular browser will decrease your chances of getting a virus.

When you enable the enhanced security measures recommended in this report, you really turn the tables in your favor. The browser with the best security features, in my opinion, is Google's Chrome.

## Google Chrome

First off, Chrome has a very clean interface that's easy to navigate. No matter what your experience level is with Internet browsing, Chrome is one of the most intuitive browsers out there. It also prevents the vast majority of pop-up ads (99%), which are not only annoying, but also sometimes dangerous to your online security.

Those are perhaps the most obvious benefits to using Chrome, but they're by no means the whole enchilada. Chrome operates in what's called a "sandbox" environment, which means that it contains all malicious viruses and spyware inside the browser, preventing them from harming your computer. If your browser gets overrun by viruses, you simply have to uninstall Chrome to get rid of the malware, then reinstall it and you're good to go.



I know what you're thinking, isn't Google working with the NSA? The answer, of course, is "classified." However, you DON'T need a Google user account to use Chrome, which severely decreases Google's ability to track your movements as you search around the web.


In fact, you can clear up your search history and browse

anonymously using Chrome's "incognito" mode. Incognito enables privacy measures such as:

- All new cookies placed on your browser will be automatically deleted when you close the window.
- Websites visited and files downloaded aren't recorded in your browsing or download histories.
- Any changes you make to your bookmarks and general settings will be saved.

### How to use "Incognito" mode:


1. Click on File
2. Select "New Incognito Window"
3. Look for the notice indicating that you've gone "incognito" (see image below)

**You've gone incognito.** Pages you view in this window won't appear in your browser history or search history, and they won't leave other traces, like cookies, on your computer after you close all open incognito windows. Any files you download or bookmarks you create will be preserved, however. 

**Going incognito doesn't affect the behavior of other people, servers, or software. Be wary of:**

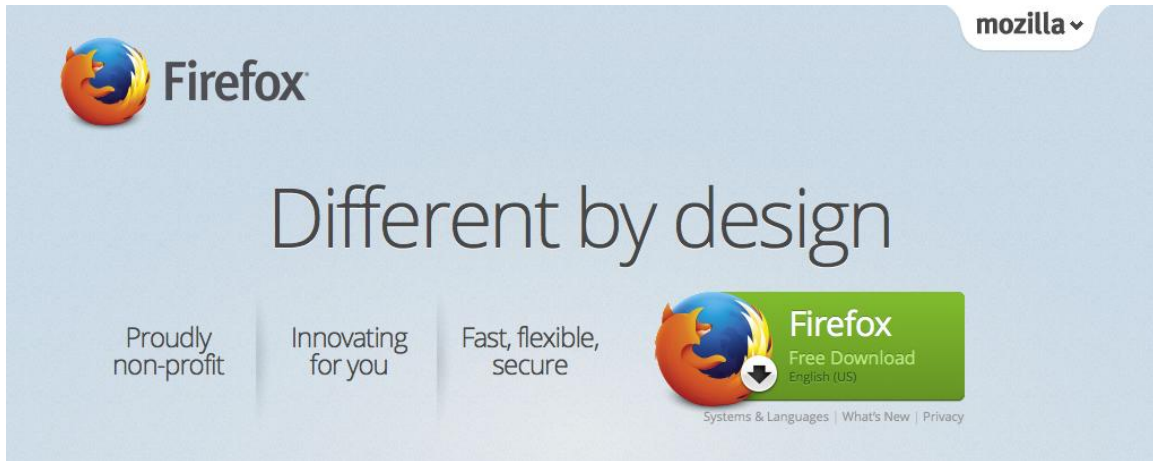
- Websites that collect or share information about you
- Internet service providers or employers that track the pages you visit
- Malicious software that tracks your keystrokes in exchange for free smileys
- Surveillance by secret agents
- People standing behind you

[Learn more](#) about incognito browsing.

 Because Google Chrome does not control how extensions handle your personal data, all extensions have been disabled for incognito windows. You can reenable them individually in the [extensions manager](#).

## Mozilla Firefox

Firefox is another great option for secure, private browsing. Like Chrome, Firefox has a private browsing option that prevents your searches, browsing, and cookies from being saved on your computer. It also works well with many add-ons that enable advanced security, such as **AdBlock** and **No Script**.



Just as it sounds, AdBlock simply prevents annoying and potentially hazardous ads from opening in your browser window. No Script prevents software scripts from running in the background of a site, which can be misused by hackers to gain access to your private data.

Firefox's "Private Window" functions much like Chrome's "Incognito" option. You simply navigate to **File > New Private Window** in order to go into a private browsing mode in which no cookies or data is saved.



## Private Browsing

Firefox won't remember any history for this window.

In a Private Browsing window, Firefox won't keep any browser history, search history, download history, web form history, cookies, or temporary internet files. However, files you download and bookmarks you make will be kept.

To stop Private Browsing, you can close this window.

**i** While this computer won't have a record of your browsing history, your internet service provider or employer can still track the pages you visit.

[Learn More](#)

## Anonymous Browsing

Neither Chrome nor Firefox allows for truly anonymous web browsing. That means your employer, local Internet service provider, and/or websites can still track what pages you visit using your IP address. They may not be able to tell who exactly is visiting these sites, but the data exists in order to track it back to your Internet connection.

The screenshot shows the Tor Project website homepage. At the top left is the Tor logo, which consists of the word 'Tor' in a stylized purple font with a purple onion bulb integrated into the letter 'o'. To the right of the logo is a navigation menu with links for 'Home', 'About Tor', 'Documentation', 'Press', 'Blog', 'Store', and 'Contact'. Below the navigation menu are three buttons: 'Download', 'Volunteer', and 'Donate'. The main content area features a large green banner with the text 'Anonymity Online' and 'Protect your privacy. Defend yourself against network surveillance and traffic analysis.' Below this text is a purple button with the text 'Download Tor' and a small download icon. To the right of the banner is a list of three bullet points: 'Tor prevents anyone from learning your location or browsing habits.', 'Tor is for web browsers, instant messaging clients, remote logins, and more.', and 'Tor is free and open source for Windows, Mac, Linux/Unix, and Android'. On the right side of the page, there is an 'Announcements' section with two entries: 'Aug 12 Three new Tor Browser releases available. 1. [Tor Browser with new Firefox 17.08ESR](#), 2. [Experimental Tor Browser 3.0alpha3](#), and 3. [Pluggable Transports Bundles](#).' and 'Aug 05 Tor security advisory: [Old Tor Browser Bundles vulnerable](#).'

If you want to take your Internet privacy to the next level, you're going to want to check out a browser named Tor. In non-technical terms, Tor is designed to jam the signal through which web users are tracked.

Tor uses a series of relays and volunteers servers to hide your information from spies and fraudsters. The only drawback is that, on account of the relays and decoys, Tor runs significantly slower than other browsers. Thus, you may want to use another browser for everyday tasks, and Tor for high-level secure browsing when necessary.

## **Best Free Anti-Virus Software**

Many viruses are not completely knock-you-over-the head obvious. In fact, some of the most harmful viruses are designed to stealthily invade your files over time. The only way to be sure your computer hasn't been compromised is to install software that will unleash a relentless, full-time search and destroy mission through your files. It must also update automatically.

Here are a few of my favorites:

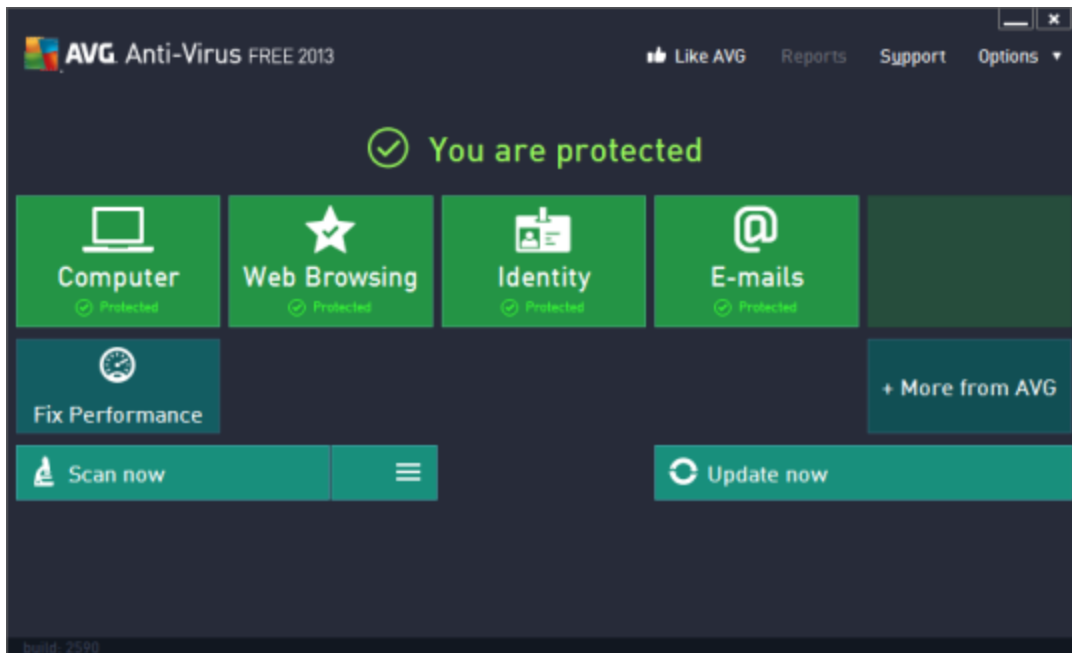
### **AVG Free**

Very few pieces of free antivirus software can boast about getting rave reviews year after year, but AVG is one of the few. AVG 2013 is intuitive and easy to use, but it's also taken a step forward in terms of privacy, which is what really wins me over.

From AVG

*“AVG AntiVirus Free 2013 also goes beyond detecting and removing viruses on your PC. Its 'AVG Do Not Track' feature gives you control over which websites can collect and use your data (available if you take AVG Security Toolbar as part of your installation). This feature joins Anti-Spyware and Wi-Fi hacker-defeating technology to deliver powerful personal protection at home or on the move.”*

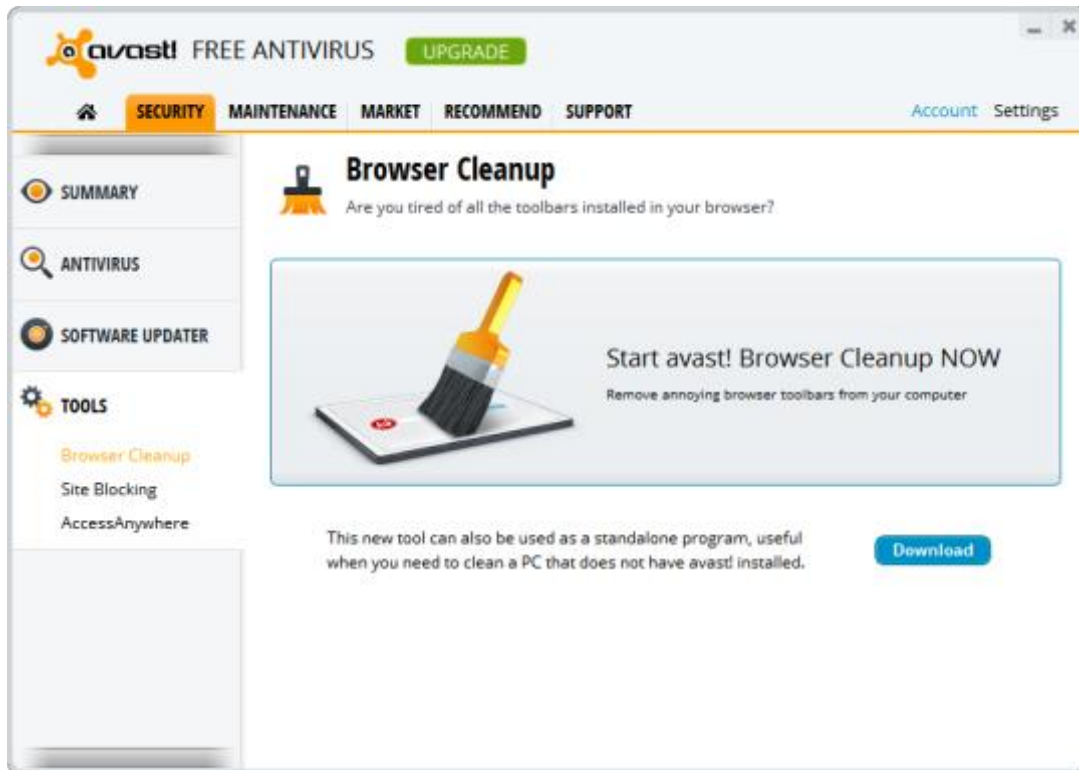




## Avast

Independent third party testing has proven that Avast is able to hold its own against other, paid antivirus programs from Symantec and Microsoft.

Even though it's free, Avast doesn't skimp on the protection it offers. It guards your computer with multiple shields, a robust set of tools, and lots of options to adjust the sensitivity level. Most importantly, Avast offers real-time protection and updates, both of which are a must in the ever-changing world of virus protection.



## What is Spyware?

Aside from viruses, there's another class of unwanted software out there that you need to be aware of and guard your machine against: Spyware. And no, the vast majority most spyware has nothing to do with the NSA or KGB...

The difference between spyware and viruses is that while viruses are designed to be destructive -- i.e. the delete or destroy your information -- spyware is designed to monitor your behavior online.

Spyware isn't always intended to annoy and harass users. Spyware is often designed by marketing companies to determine what types of products you might like to buy, or other such profitable information. Additionally, most spyware is installed **with your permission**. Typically, you install spyware programs as part of a larger piece of free software, without even knowing that it's spyware.

Eventually, this spyware starts to gunk up your computer, hogging your machine's memory and making everything run slower. And that's not a worst-case scenario. Spyware can also be exploited by hackers to steal your personal information...

## SuperAntiSpyware Free Edition

There are several good options out there, but at a cost of \$0.00, SuperAntiSpyware is a no-brainer. SuperAntiSpyware scans your computer for unwanted spyware, then displays all of the questionable files in checkboxes, so you can decide which files you'd like to delete or retain.

The "Quick Scan" option can sweep your computer in less than 5 minutes. If you feel like your computer needs some more thorough attention, you can use the "Complete Scan" function, which can take several hours.



## **Your Computer May Be Infected IF...**

Just like a virus in the real world, the earlier you detect a computer virus, the shorter the recovery period will be. Also like real-world viruses, computer viruses come in a myriad of devious forms: Trojan horses, worms, boot sector attacks, etc.

Real-time antivirus programs, such as Avast, can detect these malicious viruses as soon as they begin to act, removing them from your computer quickly and efficiently.

If you don't have antivirus software installed, or if your software is out of date, you may have virus and not even know it. Here are a few symptoms to check for:

- Your computer has become unstable and crashes often
- Unfamiliar icons appear on your toolbars (lower right hand of your screen on a PC)
- You lose control of you computer or mouse, programs open on their own, etc.
- Your computer is running slower than usual and it seems like a parasite is hogging all of your computer's resources
- You suddenly can't access drives, accessories, or printers on your network

None of these symptoms are 100% conclusive that you do have a virus, but you should take note of them when they occur. If your computer becomes 100% unusable, the best course of action is to turn it off and disconnect if from the Internet.

Then, using an uninfected computer, go online to research how to fix the problem. Some really nasty viruses may require professional help.

Click the link below to scan your system right now, without downloading any new software:

<http://www.bitdefender.com/scanner/online/free.html>

## **Secure Your Wi-Fi Connection**

In just a few short years, the Internet went from something that you physically plug into, to something that you connect to via a Wi-Fi connection.

Now, as laptops, tablets, and smartphones all share the same networks in many homes across America, the importance of securing wireless networks has reached a new level.

Hackers are known to exploit unsecured networks to do all sorts of digital mischief, but it doesn't take a high-level hacker. Any neighbor or passer-by can log into your network and potentially even access files on your computer.

Fortunately, it's fairly easy to secure a network that's under your control. You simply need to set up a password to block unwanted users from accessing your system.

Many routers these days offer encryption options, such as WPA (wireless protected access), WPA2, or WEP password protection. Use a strong password that includes a series of numbers and letters (more on strong passwords in Chapter 2).

Also, and this is a mistake I see all the time, make sure to change the SSID name of your router. This is what others in your household see when they search to log on to your network. Be sure to make it unique (e.g. not "NETGEAR"), so your guests don't log onto the wrong network by mistake.

## Public Wi-Fi Security

The wireless Internet is extremely convenient. Not only does it allow you to shop and work at the local coffee shop or bar, but you can do it from the comfort and security of your own laptop.

Still, that doesn't mean you'll enjoy the same level of protection abroad that you do on your home network. To browse safely, you'll need to adopt a public Wi-Fi protocol:

1. Make sure you're logging on to a legitimate hotspot. For example, if you're at the local Starbucks, look for a password protected network named "Starbucks Wi-Fi," not "Steve's iPhone." If you're not sure, check with the staff to make sure you're choosing the establishment's secure network.
2. Make sure your anti-virus software is updated and running properly as you browse.
3. If you allow file sharing on your home network, turn it off.

**Windows users** - Open Control Panel, then head to Network and Internet > Network and Sharing Center. Then click Choose Homegroup and Sharing Options > Change Advanced Settings. Turn off file sharing, print sharing, network discovery, and the public folder.

**Mac users** - open System Preferences > Sharing, and make sure all the boxes are unchecked.

4. Lastly, be extra careful with your most sensitive personal information when you're logged onto a public Wi-Fi network. Do you really need to log in to your Paypal account? Can that online banking session wait until you're back at home?

It's very difficult to ensure that your system is 100% secure when you're browsing in public, so it's better to avoid inputting bank passwords, credit card numbers, and social security numbers in a public setting.

## 2. How to Create Unhackable Passwords

Like your Internet connection, your passwords are on the frontlines of your online privacy. Think about it for a second; all someone needs is your username to have a chance to break into your personal accounts.

If your passwords are as bad as many I've seen, it may not take an experienced identity thief more than 3 tries to hack your account. That's because so many online users choose to protect their identities with the same, extremely generic passwords.

And in all honesty, it's the user's responsibility to create a secure password.

Here's the truth: All good hackers, whether they're from Nigeria or the NSA, know the most common password combinations. Those are what they'll try first...

According to research from the University of Maryland, the 10 most common password combinations are:

- Your user name
- Your user name followed by 123
- 123456
- password
- 1234
- 12345
- passwd
- 123
- test
- 1

If any of these passwords look familiar to you, *ahem*, you'd better go change them immediately, even if these are the passwords you use on seemingly unimportant accounts.

You see, most people don't realize how the world of identity theft truly works. Most users think that hackers go after specific targets, people with lots of cash or with whom the hack holds a grudge. Not true.

Most hackers are looking for the path of least resistance, an easy payday if you will. If you're using a simple, easy to hack password, then YOU are the path of least resistance.

Even if they hack into an old account that you no longer use, they can learn details about you that they can use to create fraudulent accounts, steal your identity, or use to con your friends and family. Remember that they're good at what they do; they're pros.

## **Password Dos and Don'ts**

Chances are, you use a variation of the same password for all of your accounts. Needless to say, this is a bad idea.

Once one of your accounts has been hacked -- email, Facebook, Amazon, etc. -- it's only a matter of time until the rest of your accounts are breached.

Here are a few tools to help you **1)** create strong passwords and **2)** store the passwords in a secure fashion.

First, on the topic of creating a password, I hope that by now you understand why obvious choices like your surname, children's names, birthdays, etc. are weak password choices (even if you combine them with the year you graduated high school).

A strong password isn't something that a friend or family member could guess. In fact, a good password isn't a word at all; it's a string of characters.

Here are a few tips for strengthening your passwords:

- Use the maximum number of characters available.
- Replace letters with symbols and numbers. For example, "Au\$t1N" instead of Austin.



- Pick strong security questions.

Even better, if you want to create a truly secure, unhackable password, it needs to be a truly random series of characters. To do this, use a random password generator like this one available through Symantec:



<http://www.pctools.com/guides/password/>

Of course, this begs the question: *How can I remember a completely random password?*

The answer is to save that password somewhere secure. For example, you might make a spreadsheet with all of your important passwords and usernames saved. This will be your master list in case a virus or unforeseen accident damages your computer.

In fact, this is the kind of critical information you'd want to keep in your bug-out bag, should you ever need to leave in a hurry during a disaster.

However, **you can't store this sensitive information in your computer!**

Instead, you should consider storing this sensitive data on an encrypted USB drive (see nearby photos) inside your fireproof box or bug-out bag.

For around \$170, the [Kanguru Defender 32 GB USB Drive](#) is one of the most respected secure thumb drives on the market. The Defender is equipped with password protection and secure file encryption. That means, even if this thumb drive were to fall into the wrong hands, there's still not a chance in hell that they're going to be able to access your files.



Another highly secure, yet slightly more budget-friendly, option is the encrypted [Corsair Padlock 2 USB Drive](#), which actually uses a padlock-style keypad to protect your drive from being accessed. It requires no extra software, just a 4-digit PIN. On top of that, it uses 256-bit data encryption so that your files are double protected.



**LastPass**

For a more practical, yet slightly less “cloak and dagger” solution, you can install a password guarding software such as LastPass into your browser’s toolbar.

LastPass remembers both websites and passwords you use for them, automatically verifying and matching them up, filling password fields automatically when you give it the “OK.” This feature is both convenient and it protects you from phishing scams.

With LastPass, you can sign in to your account from anywhere in the world where you have Internet access and retrieve all of your saved passwords. Plus, all of your password data is encrypted, so even if the files were somehow stolen, it would be useless.

I know you may be skeptical about relying on software to store and protect your most critical passwords. I was too... but after giving it a lengthy test-drive, I’ve come to reconsider.

Here’s what I’ve learned after using it for a year: LastPass allows me to use completely random auto-generated passwords to a level I never could have before.

Plus, your files are securely encrypted, meaning that even if they were stolen by a hacker, they’re complete gibberish without the codec. Also, did I mention it’s free?

<https://lastpass.com/>

LastPass \*\*\*\*\* English Sign in to LastPass

DOWNLOAD FEATURES WHY LASTPASS? SUPPORT ABOUT US ENTERPRISE

Effective, secure, and easy ★★★★★ - CNet Protects your online assets - Forbes Secure, yet dummy-proof - Lifehacker Robust security, works everywhere - Mashable

# The Last Password You'll Have to Remember!

LastPass is a password manager that makes web browsing easier and more secure.

**FREE** Download LastPass

**Get LastPass Premium!**  
(\$12 per year - that's \$1 a month!)

Windows Apple Linux HP webOS iPhone Symbian Android BlackBerry

<p><b>It's EASIER</b></p> <p>Never forget a password again and log into your sites with a single mouse click.</p>	<p><b>It's SAFER</b></p> <p>Protect yourself against phishing scams, online fraud, and malware.</p>	<p><b>It's FREE</b></p> <p>No catches or gimmicks. It's free to use on all your computers!</p>
<p><b>It's EVERYWHERE</b></p> <p>Automatically synchronizes your data; access it from anywhere at anytime.</p>	<p><b>It's SECURE</b></p> <p>All of your data is encrypted locally on your PC - only YOU can unlock it.</p>	<p><b>It's MULTI-PLATFORM</b></p> <p>Using a Mac, Windows, or Linux? LastPass works everywhere.</p>

### 3. Protect Your Inbox

Email is another major entry and exit point for sensitive information. However, unlike your browser or password data, email security entails a level of complexity that goes beyond simple hacker threats. There's a much more human element.

Yes, I'm talking about scams and email con artists. The thing about these scams is that they are very effective against people who are unaware of their existence...

We've all been conned at least once in our life, and I'll be the first to say it's humiliating. The best way to protect yourself from email scams is to learn about what scams are out there and get a basic understanding about how they work.

Typically, these scam emails use deception to get access to your most private information or to steal your money directly. Here are three of the most common email scams:

**The Lottery Scam** – In the lottery scam, a representative will contact you to let you know that, congratulations, you just won a major lottery grand prize. To collect your millions, you simply need to wire a small (in comparison to your winnings) “processing fee.”

The second you wire the processing fee (often over \$2,000), that's when the very responsive and reassuring lottery representative will disappear. If you frequently play the lottery, this scam may seem all the more convincing.

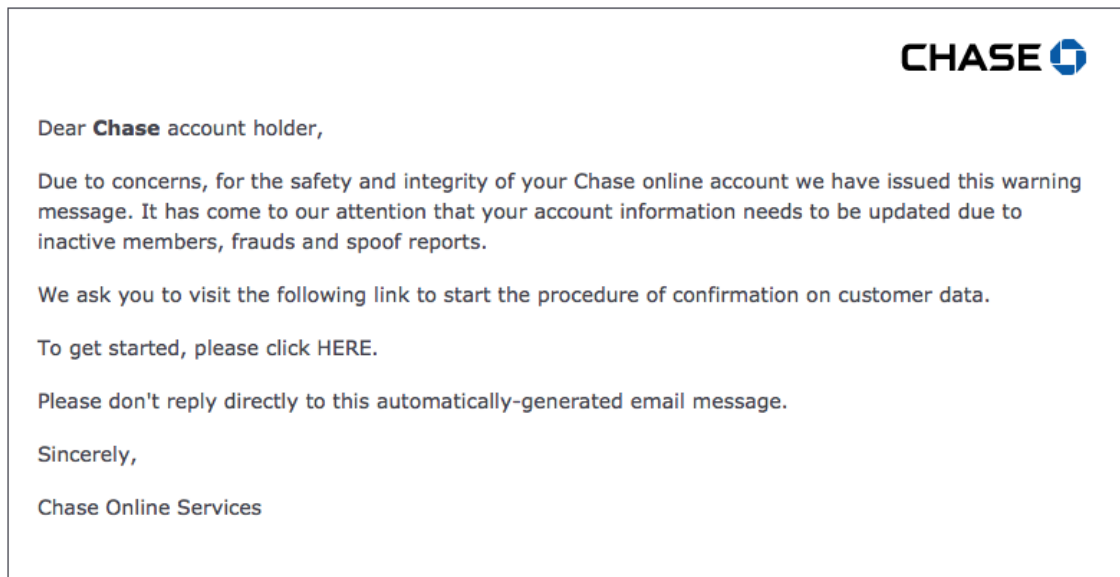
**The Bank Phishing Scam** – This scam is especially tricky, because it incorporates the idea that your online banking account has suffered a security breach. The scam email itself may claim to help you upgrade your online banking security. When, in fact, the email itself is intended to help identity thieves breach your account.

Here's how it works. You'll receive an email from someone claiming to be from your bank. Let's use Bank of America for the sake of simplicity. This email will direct you to a website where you'll be

asked to enter your username and password to “verify” or “protect your account.”

Even though the site may be designed to look like the Bank of America website, it’s a fake. When you input your credentials, they’re immediately stolen. Be wary of any such emails. It’s highly unlikely that your bank would email you this type of request in the first place. If you have any questions about the validity of an email, contact your local branch to make sure it’s authentic.

Below is an example of a phishing scam using Chase bank’s logo:



**The Job Scam** – This phishing scam works much like the banking scam, except in this scam, you’ll be offered the opportunity to apply for a fantastic and fulfilling new job. Who wouldn’t like a better-paying, more fulfilling job, right?

The email will direct you to an online form where you’ll be asked to input all of the normal job application information, along with a few extras like your SSN and driver’s license number, maybe even a credit card number to pay a nominal “processing fee.”

With all of this information, the fraudsters can begin to open new lines of credit in your name, make purchases, etc. The dangerous thing

about this scam is that you will probably never know it even happened until far too late.

## **Secure Email Tips**

It's also important to select an email provider with strong SPAM filters and scam monitoring in place. Most reputable email providers like Gmail, Hotmail, Yahoo, and Outlook will catch and filter out the vast majority of malicious emails.

By following these tips, you can drastically reduce the chances that fraudster, hackers, and Big Data can infiltrate your inbox.

1. Never download or access attachments from sender you don't recognize. This is a big one.

The subject lines of these emails may try to make it seem like you've asked for the files (e.g. "Those files you wanted"), or that they're from a friend (e.g. "Hey it's Jeff"). The scammers want you to download the attachment before you've had a chance to think. If you do, you may be downloading a serious virus.

2. Be aware that the goal of many of these emails is simply to harvest enough of your personal information (SSN, driver's license #, etc.) to commit identity theft. Never email your identity related information to an unfamiliar address, even if appears to be a job application. If you have questions about the authenticity of the email, call the company or organization to verify it.
3. Use different passwords for each of you email accounts. Even if you use auto-generated passwords, it's possible that your email account could be compromised. This ensures that even if a hacker breaches one account, the damage will be isolated to that account.
4. Never share your email passwords or give someone else access to your account. Ever. It seems obvious, I know, but it must be said.

Nobody takes your identity security as seriously as you do. So even if you trust the person with whom you share completely, you can't be sure that they won't accidentally allow a hacker through the open gate.

## Secret Agent Email Tactics

Thanks to the NSA spying scandal, we know that our email communications are not secure. In fact, the NSA is harvesting them at an alarming rate. Providers like Google, Yahoo, and others appear to be participating with the NSA's unconstitutional invasion of our privacy.

What can you do about it? Well, you have several options that will allow you to achieve 007 level email privacy:

- To transmit extremely sensitive data, you can use messages that self-destruct, just like the pros. TMWSD will enable you to share messages via email that will automatically delete themselves after it's been opened by the recipient:  
<https://www.thismessagewillselfdestruct.com/>

### TMWSD.

[ABOUT](#) | [SIGN UP](#) | [SIGN IN](#)

THIS MESSAGE WILL SELF-DESTRUCT.

TMWSD is a secure messaging service. Messages sent are encrypted, securely transferred, and automatically deleted when they are retrieved.

I accept the [terms of service](#).

PASSWORD

Optional: If set, your message will not be able to be retrieved without this password.

- Temporary email addresses are a great way to cover your tracks online. If you want to create an email account for a temporary purpose (say you're registering for some software), but you don't want to maintain the inbox, create a 10-minute



address: <http://10minutemail.com/10MinuteMail/index.html>

- If you feel that your emails are being read by anyone else (NSA, Chinese gov't, or a Romanian scam artist), you can use this service: <http://www.hide-my-ip.com/dontspyonme.shtml>

Hide-My-IP allows you to send a fake email to yourself that will reveal if the email has been opened by anyone else but you.

- You can also avoid NSA spying by creating an account with a privacy-minded email service like [RonaldReagan.com](http://RonaldReagan.com) that doesn't allow the government access to your data.

Get your Safe and Secure @Reagan.com Email today!

Site Features

- ▶ Ronald Reagan Email Login
- ▶ Message Board
- ▶ Post a Message to The Reagans 🇺🇸
- ▶ Live Chat
- ▶ Essential Reagan
- ▶ Your Reagan Story

Quote of the Day

*In this springtime of hope, some lights seem eternal; America's is.*

- Ronald Reagan

PRIVATE, CONSERVATIVE EMAIL ADDRESS

REAGAN.COM

## Opening Email Attachments

Email attachments pose a wide range of risks to your security, even when they come from a friend or relative.

The person who's sending you the attachment may not even know that the file they're sending contains a virus. Or, it's possible that their email account may have been hacked, and it's not actually the friend or relative who's sending the message.

I don't mean to sound alarmist, but these are a few of the fairly common means through which email viruses are spread.

The best way to protect yourself from these threats is to use a real-time virus scanner, such as AVG or Avast. Anti-virus programs can warn you about suspicious email attachments as you attempt to download them.

Make sure you've enabled the email scanning settings in your anti-virus software to ensure that you're protected.

**In Avast:** click Real-Time Shields > Mail Shield > Settings

**In AVG:** click Components > Email Scanner

Your second line of defense is your email service provider. Most paid email services monitor email attachments and keep up-to-date virus scanning software for liability reasons. For this reason, it's fairly rare that a virus will actually make it to in your inbox.

Lastly, to reiterate Tip #1 from the beginning of this chapter, your best and final line of defense is **YOU**...

If you don't recognize the sender, or you have a funny feeling about the message, don't download the attachment. Ignore the message until you can verify that it's legitimate, or just delete it. It's as simple as that.

## 4. Secure Online Banking and Shopping

While they may accept taxpayer bailouts and pay lousy interest rates, when it comes to online security measures the big banks are hard to beat. Few institutions have the means or the incentive to protect their data like the megabanks. The good news is that, the innovations developed for the big banks are available to many local banks and credit unions.

For that reason, online banking is not only more convenient than banking in person, but it may actually be more secure. Think about it, how hard would it be for a pickpocket to show up to a Chase bank branch and make a withdrawal?

Online banking requires passwords, IP recognition, and advanced security questions if you're signing in from an unfamiliar computer. Most reputable online banks have excellent security measures in place.

Here are a few of the state-of-the-art features that you should make sure your online bank uses:

- A secure domain (indicated by **https** instead of **http** in the URL)
- Password protection
- Data encryption
- Public and Private Key encryption

In addition to your online bank's security measures, it's also important that you use a secure browser that uses 128-bit encryption. If not, you won't be able to access most reputable banking sites.

These browsers offer 128-bit encryption:

- Google Chrome
- Internet Explorer
- Mozilla Firefox
- Safari

**On Your End...**

To ensure your online banking sessions are as secure as possible on your end, use a strong password and avoid falling victim to phishing scams.

Fraudsters can be very deceptive, creating pages that look almost identical to a bank's login area. Never follow email links that prompt you to sign in to an online banking session (see the Chase phishing scam below).

This is where software like LastPass can really come in handy. If LastPass doesn't recognize the site as your bank, that's a dead giveaway that the site your visiting may not be authentic.



Dear client of Chase Bank,

Technical services of the Chase Bank are carrying out a planned software upgrade. We earnestly ask you to visit the following link to start the procedure of confirmation on customer data.

To get started, please click the link below:

<http://www.chase.com/cmserver/users/default/confirm.cfm>

This instruction has been sent to all bank customers and is obligatory to follow.

Thank you,

Customers Support Service

## Secure Shopping Tips

Shopping online puts a world of products and information at your fingertips, things you'd never have been able to find in a store years ago are only a few clicks away. However, just as your shopping choices have expanded, so have the opportunities for fraud.

By simply following a few ground rules, many of the same ones you'd follow for telephone or credit card purchases offline, you can vastly reduce your chances of getting ripped off or your identity stolen.

- Make sure the website has recognizable trust badges and seals, such as the BBB, Verisign, Norton, etc.



- Never make purchases on sites that don't list a physical address and telephone number.
- Make sure the site is secure (https), this means the data is transmitted through a third party such as Norton and then encrypted, then sent to the seller. If that merchant doesn't have the proper software, they can't access the data you input.
- Never provide unnecessary information, such as your Social Security number or checking account number, in an online shopping transaction.
- If something seems amiss about the site you're shopping on, or if it seems too good to be true, **stop**. Do some investigating as to the legitimacy of the website. Don't risk it if something just doesn't feel right.

## Virtual Credit Card Numbers

One option that eliminates the need for added credit card security is to use a virtual (aka single use) credit card number. Several institutions offer these virtual cards as another layer of defense against fraud and identity theft.

Basically, these services work much like a prepaid credit card. You set the spending allowance and the time limit, usually valid for up to a year. You use the card for a transaction, and then the credit card number expires.

Bank of America, for example, offers a service called [ShopSafe](#). With ShopSafe, you'll be issued a 16-digit credit card number, expiration date, and security code that you can use online without giving out your real info.



## Secret Agent Trick

Here's a cool privacy tactic that most people don't know: Most online merchants only need 5 pieces of information to process a transaction:

1. Credit card number
2. Credit card expiration date
3. Credit card security code
4. Billing house number
5. Billing zip code

Notice that none of these required bits of information include the cardholder's actual name, your full home address, etc. This allows you to make virtually anonymous purchases, by providing the 5 necessary pieces of information, but creating a false name.

As long as the product your purchasing doesn't require shipping to your home, you don't have to give unnecessary details about your location. If you follow some of the offline tips I'll explain in the next

chapter, you can create an entirely fictional identity to use to make purchases, acting as an identity buffer between your online shopping and your most sensitive data.

If you're really interested in cloaking your identity from Big Brother, then you might invest a little time in selecting the details of your false identity. As long as you combine that identity with the required details to make credit card transactions, none will be the wiser.

**Example:**

Let's say this is **your real address info**:

Troy Aikman  
822 Hampton Road  
Dallas, TX 75221

Your **fictional information** could be:

David Allan Coe  
822 Skid Row Court  
Macon, GA 75221

## **5. Shielding Your Offline Privacy**

While online privacy gets most of the headlines these days, many of the old-fashioned methods continue to defraud Americans out of their hard-earned savings by the truckload.

Since many of the same forms of deception are used in both online and offline scams and identity theft, there's significant overlap in the methods you'll use to combat these attacks.

### **Monitoring Your Identity**

One of the most common ways that people learn that they've been scammed is through their credit card statements and unexpected dips in their credit score. That's why monitoring both of these records is crucial.

Most credit card companies allow their customers to challenge suspicious or fraudulent transactions. However, you must first be aware that these transactions are occurring in the first place.

Most people assume that a fraudster is going to go on a massive buying spree immediately after stealing your identity. That's not always the case. Many identity thieves make relatively small purchases (purchases you're likely to overlook) to test the water before they go big.

If you're constantly reviewing your credit card statements, you are much more likely to catch a breach before it becomes a 4 or 5 figure nightmare. Even though you may not be on the hook for any of the fraudulent charges, the experience is no walk in the park.

You can check your credit score for free using CreditKarma:

<https://www.creditkarma.com/>





## Your Credit Score Should be Free - and Now it is.

- Get Your Absolutely Free Credit Score.
- Stay on Top of All of Your Accounts in One Place.
- No Trials. No Credit Cards. Truly Free.

GET STARTED NOW

## Freeze Your Credit

Credit services are another great resource that you can use to monitor your security. The big 3 credit services each allow you to “Freeze” your credit, meaning that no one else can access your credit reports, or open lines of credit in your name without your PIN.

This is a great way to boost your security and it only takes a few minutes to do. In some states, you may have to pay a nominal \$5 fee to freeze your credit, but the peace of mind is well worth it.

Here are links to freeze your credit with each of the Big 3:

**Equifax:** <https://www.freeze.equifax.com/Freeze/>

**Experian:** <https://www.experian.com/freeze/center.html>

**Transunion:** <https://freeze.transunion.com/>




Get Answers. Take Action. \ Home \ Contact Us \ Equifax.com

**Step 1 of 3:**  
 Personal Information  Place, Temporarily Lift or Permanently Remove  Confirmation

**Place, Temporarily Lift or Permanently Remove a Security Freeze**

Welcome to the Equifax Security Freeze Website. To request a security freeze be placed, temporarily lifted, or permanently removed from your Equifax credit file please provide your personal ID information requested below. Your personal ID information will only be used for this security freeze request and will not be used for marketing purposes.



If you would like to review general information about security freezes, please [click here](#). If you would like to review State specific information about security freezes, including applicable fees for freeze services and information for ID theft victims, please [click here](#).

**Note:** If you are the victim of ID theft and have a police report or other appropriate document as required by your State, please submit your request to Equifax in writing and provide Equifax with such police report or appropriate document so you will be eligible for any benefits associated with ID theft victims.

## Postal and Delivery Security

The rise of the worldwide web has created countless new ways to be tracked, ripped off, and spied on by the NSA, but it's also created a funny loophole.

The vast majority of scammers, identity thieves, and even government spooks have focused so much energy on breaching your digital security that they've almost forgotten about actual paper mail.

With just a few simple steps, you can easily shield yourself from all kinds of malicious activity, simply by beefing up your mailbox security.

One of the best ways to foil online identity thieves is to protect your billing address. You can do this by simply using a private PO Box at the local UPS store to receive packages. These boxes are extremely secure compared to your mailbox or doorstep. Also, they can create a firewall between your billing address and your shipping address.



By combining your PO Box with the pseudonym tactic (see **Secret Agent Trick**) I described on page 28, you can receive packages and mail through your PO Box and never have these packages associated with your personal identity.

## Another Mail Trick

Never fill out a Change of Address form when you move. Contact your bank, creditors, and other important contacts directly to let them know you've moved.

Whenever you fill out one of these forms at the post office, you are entered into a database monitored by both the government and marketing firms. You're basically just telling them where they can send the junk mail or snoops.

## Subpoena the IRS

Here's one last security measure that may keep your privacy from being breached by the IRS. Most Americans aren't aware that you can file a Freedom of Information request to get a copy of the IRS's entire file on you. In fact, you can do the same thing with the FBI or NSA... if you wanna go to the trouble.



## IRS Freedom of Information



Enacted in 1966, the Freedom of Information Act, or FOIA, gives any person the right to access federal agency records or information. The FOIA is based on the presumption that the government and its information belong to the people.

A 1996 amendment to the FOIA, required federal agencies to make many types of records available online.

New law, like the OPEN Government Act, as well as new policies, such as those issued by the President and the Attorney General, promote the spirit of transparency envisioned by our founding fathers.

- [The Freedom of Information Act, 5 U.S.C. § 552](#)
- [IRS FOIA Regulations, 26 CFR § 601.702](#)
- [IRS Policy Statement 11-13](#)
- [Electronic Reading Room](#)
- [OPEN Government Act](#)
- [White House Memo on Transparency and OPEN Government](#)

<http://www.irs.gov/uac/IRS-Freedom-of-Information>

When you receive the IRS documents, you'll be able to see if you've been flagged as a non-filer or if anyone else has been receiving your refund checks (income tax refund theft has skyrocketed in the past few years).

In addition, you may be able to determine whether your returns are falling outside of the normal range, and thus that you are running the risk of being audited. For example, you may have what the IRS determines to be "excessive deductions."

By filing Form 8275 to explain why your deductions are higher than average, you may be able to save yourself from a painful tax audit. By filing Form 8275, you're show good faith, as well as providing a reason why your deductions are legitimate. Chances are good that the IRS has bigger fish to fry, so this simple filing may keep your off the radar.