HOW HACKABLE ARE YOU?

A Guide to Personal Cybersecurity

What being hacked means:

Being hacked means **your identity may be stolen**. It means your bank and investment **accounts may be robbed**. It means you may be **spied on** by the hackers who have control of your computer. This may put your children and the rest of **your family at risk**. **Your contacts may be hacked** by malware sent from your PC. Your **inbox may fill up with spam** and the ads on your web pages may direct you to **counterfeit sites**.

Your computer might be used as a malware download site or as a place to **store stolen files**. You might find all of your important **files locked** until you pay a **ransom** to the hacker. And you risk **misinformation and disinformation** attacks designed to make you **question your own judgement**.

All of us are at risk of being hacked.

Everyone is hackable: The nature of computers is such that we are always hackable. All of us. The only 100% protection is to disconnect from the Internet and turn off our computers - and that's not reasonable!

Make yourself less hackable.

By diligently doing these eight critical things, you make yourself far less hackable.

1. **Freeze your credit**
2. **Use two-factor authentication (2FA)**
3. **Careful clicking on attachments or links**
4. **Keep software up to date**
5. **Backup critical files**
6. **Install antivirus**
7. **Create passwords that are strong and unique**
8. **Encrypt your files**

SECURE THE VILLAGE

Take this quiz online!

HOW HACKABLE ARE YOU?

With the vision of a cybersecure global village, SecureTheVillage is on a mission to educate, support, and advocate for cybersecurity and data privacy. Your survey answers will guide us to improve community safety.

1. Have you frozen your credit?

- ○ Yes
- ○ No
- ○ I don't know

2. Have you set up multi-factor authentication (MFA / 2FA) on your important online accounts?

- ○ Yes
- ○ No
- ○ I don't know

3. In email, do you avoid clicking on attachments or links unless the email is expected, and you are sure of its source?

- ○ Yes
- ○ No
- ○ I don't know

4. Do you keep software (operating system, web browser, apps, ...) up to date on your computers and smartphones?

- ○ Yes
- ○ No
- ○ I don't know

5. Have you an up-to-date remote multi-version backup of personal computer and smartphone files?

- ○ Yes
- ○ No
- ○ I don't know

Take this quiz on the SecureTheVillage website so we can better direct our programs to serve and secure our Village!

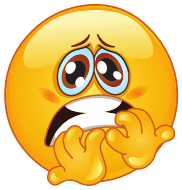
1 YES = 1 POINT!
OUT OF 5 POSSIBLE POINTS:

0 POINTS

Dangerously Vulnerable

You are not managing the basics. Your cybersecurity defenses leave you extremely vulnerable, lacking even basic defense. Get our valuable guide for eight things you can do to improve your data care.

1 POINT



Highly Vulnerable

You are not managing the basics. Your cybersecurity defenses leave you extremely vulnerable. Get our valuable guide for eight things you can do to improve your data care.

SCORE = 2

Very Vulnerable

You are not managing the basics. Your cybersecurity defenses leave you vulnerable. Get our valuable guide for eight things you can do to improve your data care.

SCORE = 3

Keep Going!

You're on your way to managing the cybersecurity basics. Get our valuable guide for eight things you can do to improve your data care.

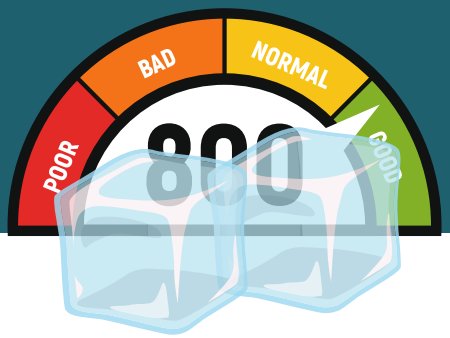
SCORE = 4

Pretty good!

SCORE = 5

Good Start!

1. FREEZE YOUR CREDIT



What to do:

Freeze your credit at the 4 credit bureaus and check your credit rating annually at each.

Why do it:

Freezing your credit is the most important thing you can do to protect your identity. Freezing your credit makes it very hard for cybercriminals to take out credit in your name and steal your identity.

If you have not frozen your credit, someone can walk into a car dealer, say they are you, present a fraudulent driver license, give them your social security number, and drive out in a new car that you are financially responsible for. If you've frozen your credit, the car dealer won't be able to pull a credit report. Without a credit report, the dealer won't sell the car to the criminal.

Credit freezes are free thanks to Federal law. You can selectively unfreeze for new credit needs from new creditors; then refreeze when their needs are satisfied. With the Equifax and other breaches, it becomes imperative to take steps to protect your identity, especially when it touches your financial resources. You do this by freezing your credit.

How to do it:

Beware - each of these companies, to varying degrees, try to upsell you to pay for a different level of protection that often does not include freezing your credit.

- **Equifax:** Go to www.equifax.com, scroll down and click on Place or Manage a Freeze. then follow the instructions.
- **Experian:** Go to www.experian.com, scroll down and click on Security Freeze, then follow instructions.
- **TransUnion:** Go to www.transunion.com, click on Resources, click on Credit Freeze and follow instructions.
- **Innovis™:** Go to www.innovis.com, scroll down and click on Security Freeze, then follow instructions.

2. USE TWO-FACTOR AUTHENTICATION (2FA)

Also known as Multi-Factor Authentication, MFA, and other similar terms

What to do:

- Set up Two-Factor Authentication (2FA) for all your online accounts, including email, banking, social media accounts, etc.
- If you're given the option, choose something other than text messaging, as text message 2FA is easier to hack than the others.

Why do it:

Two-Factor Authentication (2FA) is a Powerful Defense. Microsoft says that email is more than 99.9% less likely to be hacked if you use 2FA.

If a hacker has the password to your bank account, there may be little stopping them from getting in and stealing your money. 2FA takes care of this.

With 2FA, once you enter your password, you'll be prompted to type in a one-time passcode. The code can be sent by text, email, phone, or even using a special "authenticator" app on your phone.

Always use 2FA if it's available when accessing important online accounts. These include your email accounts, financial accounts (e.g. investments, banking, credit cards), social media accounts (e.g., Facebook, LinkedIn, Twitter), and government-related accounts (e.g. DMV, IRS, Social Security).

How to do it:

- Visit the website of every account that you want to protect with 2FA and determine if the account offers 2FA. This is often in the user-profile settings. If you can't find it, reach out to customer service.

- Check the website for each account you'd like to protect, and see if 2FA is an option. You can also reach out to customer service.

(This is where 2FA, MFA, and two-step authentication indicate the same thing. Don't be confused by similar terms indicating the same thing)

3. CAREFUL CLICKING ON ATTACHMENTS OR LINKS

What to do:

- Don't click on attachments or links in emails, unless you're expecting them.
- Be suspicious of spam, of emails and messages from friends and colleagues, and of communications from the organizations you interact with.
- Don't trust. Always verify.

Why do it:

Email is a hacker's best friend. As many as 90% of cyber attacks begin with a phishing email or text.

That email from a friend with a cartoon attached? Maybe it's from a hacker and not your friend. Open the attachment and your computer is infected. You've been hacked.

That email from the IRS, asking you to open an attachment about a possible tax penalty? It could be from a hacker. Open the attachment, and you've been hacked.

That text message from your favorite nonprofit asking for a donation? Maybe it's not from the nonprofit but from a hacker who's set up a fake website for your donation.

The email from your escrow company with wiring instructions to close on that house you're buying? Maybe it's not from your escrow company. Maybe it's a hacker hoping you'll wire your bank loan to them.

How to do it:

When it comes to protecting yourself from email and text message attacks, the rule is simple: Don't trust. Always verify.

Call your friend. Go to the nonprofit's website and make your donation there. Ignore the fake IRS email along with similar emails designed to look like they're from your bank or other businesses.

And always make that phone call to double-check the authenticity of a request to wire money.

Here are some tips to help manage dangerous emails or texts:

- Look for misspellings in words or links. Hover your mouse over links and usually, a pop-up will display the actual website or email address you're being lured to
- When sharing a link or file, add a personal touch so the recipient knows it's from you
- Forward any phishing emails to reportphishing@apwg.org
- Copy and paste phony texts to 7726 to alert your cell phone provider

4. KEEP SOFTWARE UP TO DATE

What to do:

Keep software up to date on all your devices. This includes your Windows or Mac operating system, your web browsers, your word processors, your spreadsheet programs, your PDF readers, iTunes, Zoom, and all the other applications on your computer and smartphone.

Why do it:

As we know so well when our computers and smartphones freeze up, the programs we run on our computers are not perfect. This makes them the "hacker's playground."

Cybercriminals look for bugs in programs. Bugs are mistakes in the code that the programmers made when writing the software. Often, the software will look and work just fine to you and me, but cybercriminals know how to use bugs to affect security. When cybercriminals find bugs, they write other programs to "exploit" these bugs. It is these exploits that they use to hack your computers and smartphones.

When software companies discover a bug in their programs, they "patch" the program, fixing the bug, and release an update that is no longer vulnerable to the hacker's exploit.

Software companies fixed 28,000 vulnerabilities in 2021.This is 50% greater than the 18,000 vulnerabilities in 2020 and double the 14,000 in 2017.

This is why it's so important to keep all the software on your computers and smartphones updated with the latest versions of the programs you're using.

How to do it:

- Some software is designed to automatically update. Microsoft, for example, is designed to update automatically when updates are released on the 2nd Tuesday of each month.
- Firefox and Chrome also update automatically when you shut them down and restart them. They may not update though if you don't restart them.
- You can update the programs on your iPhone by going to the App Store and checking for "available updates." The Android offers similar update management.
- SecureTheVillage publishes our *Weekend Patch & Update Report* every Sunday to help residents and small businesses keep their computer updated. We publish it on our website, and on our LinkedIn and Twitter accounts. It's also available by email bundled with our *Cybersecurity News of the Week*. Simply visit https://securethevillage.org/, scroll down and page and select "Join Our Email List."

5. BACKUP CRITICAL FILES

What to do:

Maintain a remote, multi-version backup of personal computer and smartphone files.

Why do it:

We have a friend whose smart phone was stolen while she was shopping. Her phone was not backed up and she lost over 5,000 photos of her grandchildren. It was heart-breaking.

Backing up your files means you can get them back if something happens to the originals. This includes device theft or loss, hard drive failures, earthquakes, ransomware attacks, and data overflow.

How to do it:

There are several different ways to back-up your files, each its own pluses and minuses.

The simplest way — old fashioned by today's standards — to back up the files on your computer is to connect a USB-drive or auxiliary hard drive to it. Both Windows and Mac provide built-in tools for doing this. While simple, this strategy doesn't protect you if there's a fire or earthquake that destroys your computer and backup. That's why people who use this strategy are encouraged to take their backup to a different location.

A better — more modern strategy — is to back up to the cloud. There are two ways this is done.

One form of backup continuously synchronizes each file on your computer with a corresponding backup file in the cloud. An advantage of this method over backing up to a USB-drive is that you can work on a file on your home computer and then continue working on the file from your laptop when you're away. Office 365 is an example of a program that synchronizes files between your computer and the cloud. The disadvantage of a synchronous cloud backup program, however, is that it doesn't protect you against ransomware and other destructive attacks. As the ransomware encrypts files on your hard drive, these encrypted files now over-write their cloud copies.

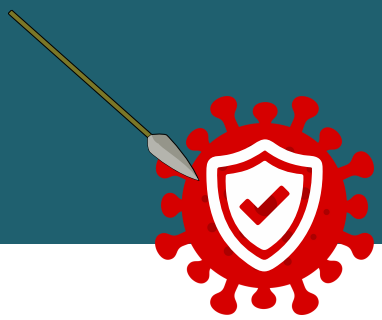
This is why the best form of cloud backup synchronizes your files AND maintains older versions of your files as well. Rather than overwriting the cloud backup when the computer file changes, these programs keep the old backup file and create a new copy of the file. This way if the new file becomes unavailable because of ransomware, the older versions will still be available. It also means if you make a mistake in a file, you can return to an earlier version of the file and fix it. Apple's iCloud and Microsoft's OneDrive, as well as commercial offerings like Carbonite™, provide this more advanced backup strategy.

Your smartphone's tools can be set to back up to the cloud or to your computer. Don't be afraid to check the documentation.

Whatever backup strategy you use, make sure your backups are encrypted.

You also want to test your ability to recover files from your backups. You don't want that feeling in the pit of your stomach you get when you discover your backups aren't any good.

6. INSTALL ANTIVIRUS



What to do:

Install antivirus on personal computer(s) and smartphone(s) and run it continuously.

Why do it:

Hackers create and use computer viruses to hack computers and smartphones. Once a virus infects your device, the hacker has control. Computer viruses and other kinds of malware (malicious software) enable the hacker to steal your information, destroy your data, and turn your computer into a "bot" under his control.

Modern antivirus programs are designed to block viruses and other kinds of malware from running on your devices. They can also search your hard drive for the telltale signs of a virus intrusion, removing what it finds.

An important caveat: While antivirus software is necessary, it is not sufficient. Antivirus programs work by comparing a file against a database of known malware, much the way law enforcement might compare a suspect against a photo gallery of known criminals. This only works if the malware is in the "gallery of known malware." With 500,000 new malware variants being created every day, it's not hard to see that antivirus programs are playing from behind.

How to do it:

- Most modern personal computer operating systems offer, as standard, a suite of security and privacy functions, including an antivirus program. In addition to the antivirus program Defender, the Windows® suite includes features such as access control, firewall, backup, parental control and storage/disk tune-up. The MacOS® offers XProtect for antivirus together with access control, backup (Time Machine), firewall, storage tuneup, and location control.
- Apple provides a basic antivirus program as part of iOS for the iPhone and iPad. Google provides a modicum of antivirus protection on Androids. Android users should also be cautious to only install programs from the Google Store and to run Google Play Protect.
- There are also numerous commercial offerings from companies such as Norton, McAfee and Bitdefender. Some commercial suites include additional functions, such as a password manager and a VPN.
- How to use your antivirus software:
    - Run a full scan at least weekly on your computer. This may be set by default. If not, you can initiate the scan manually. Check the help system.
    - You should also initiate a manual scan if a virus infection is suspected. Keep in mind though that the antivirus program is best at identifying known viruses. If it identifies a virus, it will likely be able to remove it. Just because it doesn't identify a virus, though, doesn't mean you don't have one.

7. CREATE PASSWORDS THAT ARE STRONG AND UNIQUE

What to do:

Create long, complex, unique passwords for each online account.

Why do it:

Passwords provide a measure of protection from hackers.

Short, guessable passwords are an open door for hackers. Hackers are way too sophisticated to sit at their computer trying to guess your password, one guess at a time. Hackers have lists of common passwords that people use, like “password” and “123456.” They have dictionary lists of every word in several different languages. And they have access to more than a billion passwords stolen in other data breaches. Hackers run programs that try every password on their lists, knowing that in many cases, they will be successful in finding your password and taking over your account.

Once the hacker knows your password to an account, the hacker can take over the account if it isn’t protected with Two-Factor Authentication (See Rule 2). If that same password is used on other sites, then the hacker can take over these other sites. If a hacker knows the password to your favorite shopping site and that password is the same as the password to your bank, then the hacker knows the password to your bank.

How to do it:

Your passwords are the “Keys to the Kingdom."

Long, complex, unique passwords:

- Modern password recommendations advise users to create long complex “passphrases.”
- Here are some examples of long complex passphrases:
  - Long: 12 or more characters
  - Complex: 3 of 4 lower case, upper case, numbers, and special characters
- Long and complex passwords are useful:
  - 1Hate$Passwords
  - Hello7Goodby$%
  - 123456789Gy&
- Passwords on accounts having 2FA only need to be changed when a breach of that site occurs, not on any regular schedule.
- Passwords on accounts with information you care about that don’t have 2FA should be changed at least annually or anytime a breach is announced.
- Be especially careful with passwords for your financial accounts, particularly those that don’t have 2FA. Make doubly certain these are long, complex, and unique.

Storing your passwords:

- Don't store your passwords in a file on your computer or smartphone, even if you think it's protected.
- If you must write down your passwords, be sure to store them as safely as you would your wallet.
- Storing multiple passwords with a password manager:
  - If you have more than just a few passwords, you will want to use a password manager to keep track of them.
  - Use a password manager with 2FA
  - Use a password for your password manager with at least 16 characters.

8. ENCRYPT YOUR FILES

What to do:

Encrypt your files on your computers, smart devices, portable storage, and the cloud.

Why do it:

When you encrypt your files, you make them unreadable to anyone who doesn't have the encryption key. Encrypting your files prevents someone from learning your personal secrets, financial information, and the like. Encrypting your files keeps this sensitive information secret were a hacker to steal your device.

Because they are small and easy to lose, portable storage, like USB flash drives, are particularly dangerous and need to be encrypted.

A recent story tells of a government worker who had the personal information of an entire city's population on an unencrypted flash drive. The worker planned to take the flash drive home to work on it. Before going home, however, he stopped in a bar where he apparently had too much to drink. Several hours later he woke up. The flash drive was gone, putting the entire city's population at risk of identity theft.

How to do it:

- Both major personal computer flavors – Windows and Mac – support file encryption on fixed and external disks (e.g. flash drives). Use BitLocker® (for Windows) or FileVault® (for macOS). Make sure you safeguard the encryption key. Write it down, describe what it's for, and store it someplace that's physically secure.
- Once you have passwords set on them, the iPhone and Android smartphones will encrypt your smartphone data by default.
- Many cloud storage providers also encrypt your data by default. You will want to make sure that encryption is enabled in the cloud.

About Us

SecureTheVillage is on a mission to educate, support, and advocate for cybersecurity and data privacy. We connect cybersecurity leaders to accelerate progress toward a secure global village. We work in hard-problem areas, including helping families keep themselves safe in cyberspace. To learn more, please visit SecureTheVillage/meet-us.

This guide is for "residents" of the global village, for everyone who might feel insecure in their online activities. It is intended to provide enough background, explanation, and "how-to" details to enable you to protect yourself against the most common, serious risks when using the internet.

Further Reading

An extensive set of references for village residents is available at: https://securethevillage.org/cybersecurity-for-individuals-families.

CyberGuardian: a SecureTheVillage Guide for Residents, written by SecureTheVillage Board member, Dr. Steve Krantz, is available on Amazon.

****

SECURE THE VILLAGE

Platinum Partner

MILLER KAPLAN