

SECURITY CHECKLIST



Home Internet Security Course



Tools and tips to keep your family safe online

Passwords

Always use **strong passwords** on the Internet. A strong password is one that is hard for someone else to guess.

Kevin Mitnick's 10 Rules for Stronger Passwords

- ☐ Don't tell your passwords to anyone! *Nobody* should ask for your passwords, and you should never give your passwords to *anyone*. Normally, tech support does not need your password to get into your account, so there's no reason for a legitimate tech support person to ever ask for your password.
- ☐ Don't use simple dictionary words, pets' names, or people's names for passwords. Avoid easy-to-guess numbers, such as your age, zip code, birthday, or anniversary.
- ☐ Use passwords that are at least 20 characters long. And do not write them down where they can be easily found.
- ☐ Create a "pass phrase" instead of just one word (for example, *\$3 for the pirate hat*). Or think up a few nonsense words that you can remember easily (for example, *Betty was smoking tires and playing tuna fish*).

"It's important to keep malware (malicious software) off your computer so hackers cannot intercept your passwords."

"Even if your passwords are very strong and hard-to-guess, malware can still allow a hacker to get them."

KEVIN MITNICK

- ☐ Use a different password for each website. Do not use simple patterns like "password1" "password2", "password3" or "amazon4me", "netflix4me", "yahoo4me" for different sites – those are too easy to guess.
- ☐ Change your passwords for sensitive web sites (such as your online banking) every 60-90 days. Do not use easy-to-guess patterns when you change them.
- ☐ If you think someone may have learned your password, change it immediately. Then check the websites where you use that password for any signs of misuse – starting with your online banking site.
- ☐ Sometimes websites ask you to enter the answer for a "security question" you can use if you forget your password. Make your answer to the security question just as hard to guess as your password.
- ☐ If your bank or webmail offers you extra security features, use them!
- ☐ Consider using a password manager such as **KeePass** or **Password Safe**. Password managers make your Internet use a lot safer and easier.

Giving Out Personal Information

Criminals can use your personal information to harm you – to steal your money, steal your identity, and ruin your reputation and your credit.

Even if someone *tells* you they are from your bank or your credit card company, you should *never* reveal this kind of information to anyone unless *you* started the contact, and you *know* you are talking to a legitimate organization.

Stop – Look– Think before you give out personal information

- ☐ Be careful when you get an automated phone call with a recording that asks you to verify your identity, your credit card number or other personal information. *Do not provide that information!*
- ☐ Do not trust *any* telephone numbers you are sent in an email. Use Google to look up the real phone number you need to call, then *you* call *them*.
- ☐ Don't ever give out your Social Security number unless there is a legal requirement to do so.
- ☐ Don't respond to *anyone* asking for personal information through social media like Facebook, email, text or phone for information like your Social Security number, bank account number, date of birth, address, or driver's license number unless *you* initiated the contact to a number or website you can verify.
- ☐ Consider using an identity theft notification service that alerts you if your (or your children's) personal information is posted on the Internet.

“You can safely give out personal information if YOU contact an organization that you have some business with, and they have a legitimate need to ask for that information.”

“But always suspect a problem if THEY contact YOU in a way you cannot verify.”

KEVIN MITNICK

What is “personal information”?

Personal information is defined as: **First name** (or first initial) AND **last name** AND **at least one** of these items:

- | | | |
|---|---|---|
| • Social Security # | • PINs or passwords | • Vehicle identifiers and serial #s, including license plate #s |
| • Driver license or state-issued ID # | • Password challenge question responses | • Medical histories |
| • Military ID # | • Account balances or histories | • National or ethnic origin |
| • Passport # | • Wage and salary information | • Religious affiliation(s) |
| • Credit card (or debit card) #, security code, and expiration date | • Tax filing status | • Physical characteristics (height, weight, hair/eye color, etc.) |
| • Financial account #s (with or without access codes or passwords) | • Biometric data that can be used to identify an individual, (e.g., finger or voice prints) | • Insurance policy #s |
| • Customer account #s | • Digital or physical copies of handwritten signature | • Credit or payment history data |
| • Unlisted telephone #s | • Email addresses | • Full face photographic images |
| • Date or place of birth | • Medical record #s | • Certificate/license #s |
| • Mother's maiden name | | • Internet Protocol (IP) address #s |

Online Banking

Online banking is very convenient, but it carries greater risks than many other types of Internet activities. You can protect yourself from these risks by taking special precautions with your online bank accounts.

Questions to ask your bank or credit union

- What is my liability if someone accesses my online bank account? Am I insured against fraud and theft?
- Do you offer 2-factor authentication? This is a service that sends you an additional code via text message to your mobile phone. To log into your account, you need both your password *and* the code that was sent to your mobile phone.
- Can you disable outbound wire transfers from my accounts?
- Can you confirm with me by telephone before any wire transfers go out from my accounts?
- Can you enable alerts for any transactions greater than an amount that I specify?

If your financial institution *does* offer these extra security options, *be sure to take advantage of them!* If they *do not* offer these protections, consider moving to another financial institution that does.

“Criminals can create a very realistic webpage that looks almost exactly like your real banking site.

“That’s why it is dangerous to click on links or to open attachments in emails that look like they come from your bank or your credit union.”

KEVIN MITNICK

Tips so you DO NOT get tricked

- ☐ Use a bookmark or the address bar in your web browser to go to your banking site.
- ☐ Never click on links in any email or website you aren’t sure about.
- ☐ Beware of email attachments you were not expecting.
- ☐ Do not trust the phone number sent in any emails. Get your financial institution’s phone number from the back of your credit card, or by going to their website for it.
- ☐ Set alerts for adding new bill pay vendors or for debits in excess of a specified amount.
- ☐ Audit your online transactions frequently – once a week is recommended.
- ☐ Download a secure browser like Google Chrome. Use that browser for your online financial transactions and to look at email attachments safely, using the VIEW option.
- ☐ Make sure you practice good password management.
- ☐ Keep your operating system, your desktop applications, and your Internet security software up-to-date.

Protecting Children Online

Tips for keeping younger children safe online

- ☐ Talk with your kids about online safety and the dangers of communicating with strangers.
- ☐ Put the computer your children use in a public part of your house so you can supervise their Internet access. Act immediately if they seem to be hiding something from you.
- ☐ Limit children's Internet access to a set amount of time each day, with a regular schedule.
- ☐ Teach them *never* to use their real name, address or school name for an avatar.
- ☐ Teach them *never* to agree to meet someone in the real world whom they met online, and to tell you *immediately* if someone wants to meet them in the real world.
- ☐ Set up an account on sites your child visits, and 'friend' your child. Become a positive part of their online world.
- ☐ Switch 'open chat' off until you are sure your child is mature enough to use it appropriately.

Parents and teens should be aware of the ways older teens can get in serious trouble on the Internet

- Downloading movies or music illegally.
- Visiting porn sites that put malware on your computer.
- Engaging in cyber bullying.
- Sexting (sending and receiving inappropriate pictures).
- Posting inappropriate pictures of themselves or others on social media sites.
- Getting involved with online hate sites.
- Becoming part of an online 'hacktivists' group to attack public websites. Your PC is not anonymous and can be tracked.
- Experimenting with illegal hacking. It may start as just a challenge, but it's a way teens can get in very serious trouble.

“Be aware of what your kids are doing online. Talk to them about the consequences of these activities.”

“Let them know you are monitoring their PC use. And then do it - take the time to monitor their PC.”

KEVIN MITNICK

Technical tips for parents

- ☐ Kids should use a separate computer. They tend to download carelessly, and infect that computer with malware.
- ☐ We suggest that you use a parental control software product and monitoring software like **eBlaster** from SpectorSoft to help protect children online.
- ☐ Computers use a service called DNS to link your web browser to Internet sites. We recommend **OpenDNS**, a free DNS provider that creates an extra security filter that scans the Internet for inappropriate sites, and has built-in parental controls. Visit opendns.com to learn more and for instructions how to change your current DNS to OpenDNS.

Protecting Your Identity

When Internet thieves steal your identity, they steal your time, your money, and your good reputation.

Kevin Mitnick's tips for protecting your identity online

- ☐ Keep all documents with information that can identify you out of view of both friends and strangers.
NOTE: Most identity thieves are people who are close to you.
- ☐ Use a good quality cross-shredder when you dispose of any documents that contain personal information.
- ☐ Contact your financial institution immediately if you do not receive your bank or credit card statement.
- ☐ Carefully review your credit card and bank statements every month for fraudulent transactions. Call your financial institution immediately if you find any.

***“If thieves steal your MONEY, that is bad.
But if they steal your IDENTITY,
that’s MUCH worse!”***

KEVIN MITNICK

- ☐ Obtain your credit report from all three credit bureaus (Experian, Transunion, and Equifax) at least once a year to check for unauthorized entries.
- ☐ Place free fraud alerts with all three credit bureaus so every credit request must first be verified. A fraud alert is something that the major credit bureaus attach to your credit report. When you (or someone else) tries to open up a credit account by getting a new credit card, car loan, cell phone, etc., the lender should contact you by phone to verify that you do want to open a new account. If you aren't reachable by phone, the credit account should not be opened.
- ☐ Opt out of sharing your nonpublic personal information or credit report information with other businesses.
- ☐ Consider using a credit protection service to get alerts if someone applies for a new extension of credit in your name.
- ☐ *Never* give out your Social Security number and/or your date of birth to anyone unless you initiated the contact and you are legally required to provide that information.
- ☐ Review your Social Security Earnings and Benefits Statement to be sure that your yearly salary is correct.
- ☐ If you provide identity information on an Internet site, first verify that the site is legitimate. Google the name to get the correct website address or phone number.
- ☐ Beware of phishing attacks that may be used to steal your information. You can learn more about phishing attacks in the “Opening Email and Attachments” section of this training.
- ☐ Consider setting up electronic alerts on your bank and credit card accounts to send a text message to your mobile phone under several conditions, such as a transaction that exceeds \$200.
- ☐ If you are on a wireless (Wi-Fi) network and you visit websites that require personal information, make sure that the wireless network is encrypted. (It shows a little lock and requires a password to get in.) Open wireless networks in public places may allow attackers to intercept your passwords under certain circumstances. Never conduct *any* transactions that require confidential information on open wireless networks.

Securing Your Computer and Home Network

If you want to have a secure home network, you need to keep your computers up-to-date.

Kevin Mitnick's tips for protecting your identity online

- ☐ If you run Windows, set your computer to automatically update the operating system, so that your PC or laptop will always have the latest updates. To learn how to turn on automatic updates, see Microsoft's support website: <http://support.microsoft.com/kb/306525>
- ☐ Make sure all your applications are updated automatically. Many people tend to forget this, leaving their systems vulnerable to malicious attacks.
- ☐ Make sure that your antivirus software has not expired, and that the latest antivirus definitions are being downloaded every day. Check your antivirus software and make sure that the definitions are up-to-date.
- ☐ If you use a wireless network, set an encryption password on your wireless router. Encryption requires you to enter a password before a device can use your network to access the Internet. This helps stop criminals from "piggybacking" and using your wireless network for their own purposes.
- ☐ Currently, WPA2 is the most secure encryption protocol for wireless routers.*
- ☐ Make sure that the firewall in your wireless router is turned ON, and that you change the administrator password to a strong password that no one else can guess.
- ☐ Wireless routers have software (firmware) that can become out-of-date. Update this once every six months. If you do not know how to update the firmware in your router, ask a knowledgeable friend.

**If you do not know how to set a WPA2 password, find the manufacturer's name and model number on your wireless router. Then Google that router information and "set WPA2 password" to find instructions. Or you can ask a knowledgeable friend or contact a service such as Geek Squad.*

"Securing your computer and your network is VERY IMPORTANT!"

"If you do not know how to update your system and applications, or how to set an encryption password on your wireless router, ask a knowledgeable friend to help you."

KEVIN MITNICK

Spam, Viruses and More...

Spam is often the carrier for all kinds of viruses and other malicious code that can infect your computer.

For example, malware such as “trojans” can create a “backdoor” in your computer that criminals can use to completely take over your computer! That’s why it is so important to make sure that your computer *does not get infected*.

Tips to protect from spam and viruses

- ☐ *Think before you click.* Stop and look at each email and consider if it might be dangerous. Your spam filter might not have caught a malicious spam message. *Do not click on any link or open any attachment* in an email you think may be dangerous.
- ☐ If you are still using Windows XP, upgrade to at least Windows 7 or 8 because Windows XP is very easy to hack.

“You may want to consider purchasing a full Internet Security suite that will enable automatic updates, eliminate spam, and provide a robust 2-way firewall.”

KEVIN MITNICK

- ☐ Install a good Internet security product.
- ☐ Back up your data and applications frequently. If you can, set up your system for automatic backup.
- ☐ Configure your operating system updates to download and install automatically.
- ☐ Do not log in as an Administrator for your day-to-day computer use. Log in as a Standard Account instead. That blocks most of the malware that tries to install itself.
- ☐ If you have children, create Standard User Accounts for them to use. This link to Microsoft’s website shows you how to do that: <http://windows.microsoft.com/en-US/windows7/Create-a-user-account>
- ☐ Use a software tool to regularly update software that you installed after you bought the computer. This is called ‘patch management’.
- ☐ Consider using a paid service to provide stronger protection against spam. Google “services that eliminate spam” to learn more.
- ☐ Windows comes with a free firewall. But if you’re an advanced user, you could consider installing a more robust 2-way firewall that requires your permission for all *outbound* traffic as well as inbound.

Opening Email and Attachments

Here are some terms you should know

Spam

Email or text messages you get on your PC or phone that you did not ask for.

Phishing

Phishing email tries to make you click on something, fill out fake forms or open a malicious attachment.

Spear-phishing

Phishing that is specifically targeted to you. They send an email that looks like it comes from someone you know.

Social engineering

The art of manipulating, influencing or deceiving you in order to gain control over your computer system. Phishing and spear-phishing are both forms of social engineering.

“If you open an infected attachment or click a bad link, criminals can take full control of your computer and use it to commit crimes.

“They can record everything you type – including your online banking login information.

“They can listen to you via the microphone on your computer.

“And they can even spy on you with your computer’s webcam!”

KEVIN MITNICK

Look for the red flags!

Before you open any attachment or click on any link in an email, look closely at each of these parts of the email:

- ☐ The **From:** line
- ☐ The **To:** line
- ☐ The **Date:** line
- ☐ The **Subject:** line
- ☐ **Attachments**
- ☐ The **content of the message** itself
- ☐ And any **hyperlinks** they want you to click

Carefully check each of these areas before you click on any link or open any attachment in any email.

Download *Social Engineering Red Flags* from the Resources tab at the top of the Main Menu. It lists the questions you should ask yourself when you examine an incoming email.