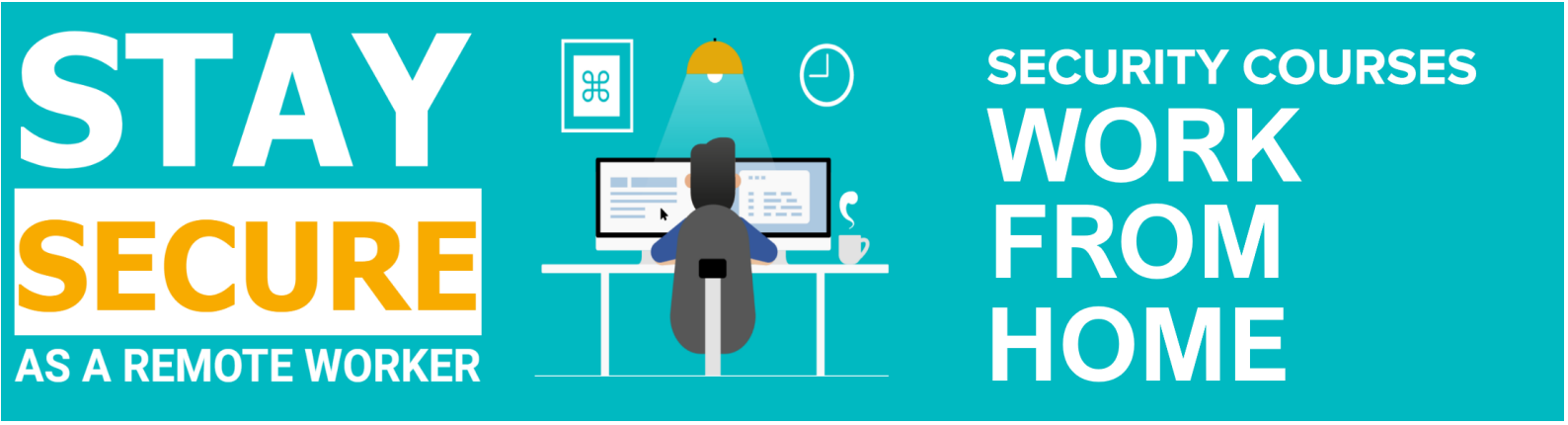


KEEP YOUR PC SAFE WITH THESE CYBERSECURITY TIPS FROM LUCY SECURITY

Whether you use your PC primarily for work or personal computing, you want to keep it and its contents secure. Take these steps to lower the risk of having your computer compromised.

✓ TIP 1: KEEP ALL SOFTWARE UP TO DATE

Many security problems are caused by software which does not have the latest updates installed. Most software can install updates automatically. If you are working on a Windows PC, make sure to turn on automatic updates to keep Windows, Microsoft Office, and other Microsoft applications up to date.

Turn on Automatic updates also for non-Microsoft applications like Adobe Acrobat Reader and other programs you regularly use.

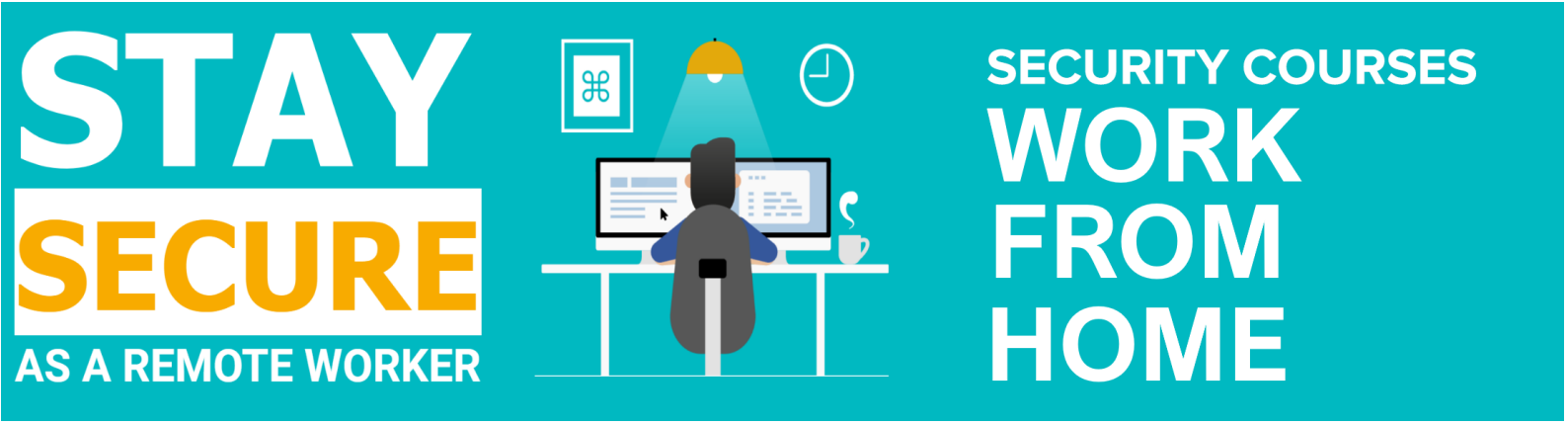
For Macs, use the software update mechanism which can be found in System Preferences under the Apple menu.

✓ TIP 2: INSTALL ANTI-VIRUS SOFTWARE

Anti-virus software is a must for everyone – Windows as well Mac users. Anti-virus applications also have to be updated regularly. If you use USB thumb drives or external hard drives, always scan them for viruses—particularly if the drive belongs to someone else.

✓ TIP 3: BROWSE THE WEB SAFELY

Avoid visiting sites that offer potentially illicit content. Especially don't visit Porn Sites (or any other shady website)! The problem is that there are sites out there designed to infect your computer with a virus. Many porn sites target you deliberately. Use a modern browser like Microsoft Edge or the latest Chrome version, which can help block malicious websites and prevent malicious code from running on your computer. Never download, install, or run any software from non-trusted sources.



✓ TIP 4: SECURE E-MAIL USAGE

When you check your email, beware of scams that try to steal your personal information or your money. Many of these scams are known as "phishing scams". Don't open suspicious attachments or click unusual links in messages. They can appear in email, tweets, posts, online ads, messages, or attachments, and sometimes disguise themselves as known and trusted sources.

✓ TIP 5: CREATE YOUR OWN USER ACCOUNT WITH LIMITED USER RIGHTS

Even if you're the only person who uses your computer, set up a user account without Administrator privileges from which you work. This restricts the damage malicious software can do.

✓ TIP 6: KEEP YOUR PASSWORD SAFE AND HARD TO GUESS

Use a password that has at least eight characters and a combination of numbers, upper- and lowercase letters. Don't use recognizable words or combinations that represent birthdays or other information that can be connected to you. Also use a different password for each website you use.

✓ TIP 7: CHECK YOUR FIREWALL

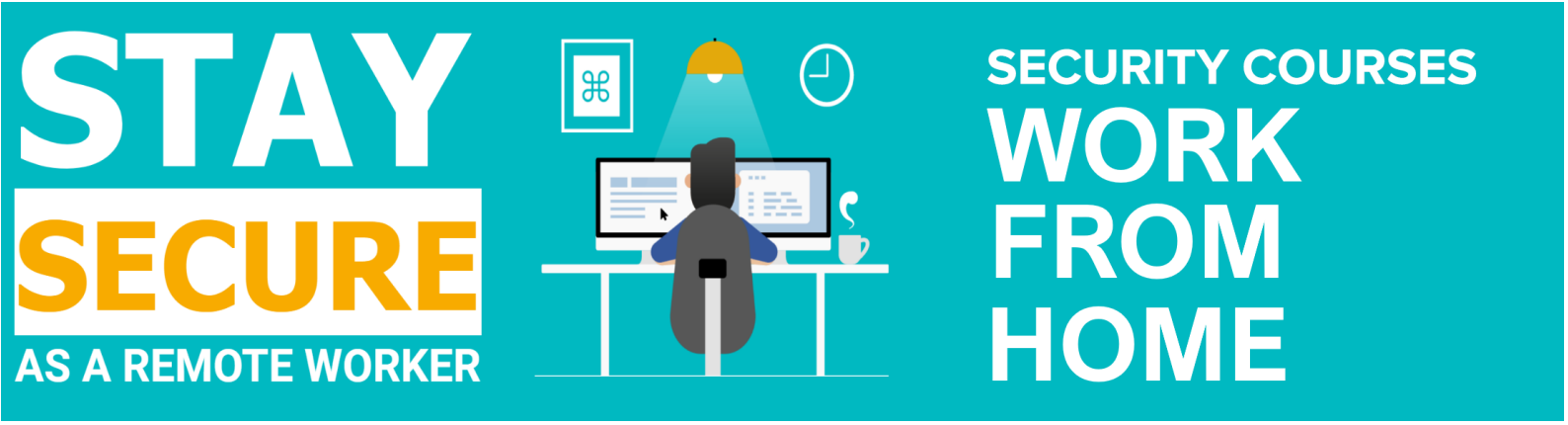
A firewall acts as a barrier between your computer or network and the internet. Checking your firewall sounds complicated, but it really isn't. If you own a Windows-based system, just go to your control panel and type "firewall" in the search box. If your firewall is "on" or "connected," then you're good to go.

If you own a Mac, click the Apple icon on your toolbar, go to "System Preferences," then "Security & Privacy" then "Firewall."

✓ TIP 8: AVOID RISKY PERIPHERALS

USBs and other storage mediums can be packed with malware. Do not use USBs or other external devices unless you own them

To avoid infection by malware and viruses, ensure that all external devices either belong to you or come from a trusted source.



✓ TIP 9: DISCONNECT FROM THE INTERNET WHEN NOT IN USE

Turn off your computer overnight or during long stretches of time when you're not working. Always being on makes your computer more visible target for hackers. Shutting down breaks the connection a hacker may have established with your network and disrupts any possible mischief.

✓ TIP 10: SEPARATE BUSINESS FROM PERSONAL ACTIVITIES ON YOUR PC

When computers are used for personal rather than professional use, the chance of infections and other security incidents increases—movies, games, music and other personal applications all have associated risks. If you own only one PC and you want to separate your work and personal activities, take the time to create different user accounts—one for your work and one for personal use.

✓ TIP 11: SECURE YOUR HOME NETWORK

It's important to secure your home Wi-Fi. Make sure your home Wi-Fi has security enabled and that you've changed your router's administrative password. Most routers also let you 'hide' your Wi-Fi too, which means people need to know both the Wi-Fi ID and the password to get online.

Now you know the important steps you need to take to secure your personal and company information when working on your private PC. Stay safe!