Security for Humans

Because we are the problem

Ways Things Go Sideways

Security Risks for Computers

Adware

a type of software that downloads or displays unwanted ads when a user is online or redirects search requests to certain advertising websites.

Botnets

Botnets are networks of computers infected by malware and controlled remotely by cybercriminals, usually for financial gain or to launch attacks on websites or networks.

Many botnets are designed to harvest data, such as passwords, Social Security numbers, credit card numbers, and other personal information.

Ransomware

A type of malware that infects a computer and restricts access to it until a ransom is paid by the user to unlock it. Even when a victim pays the ransom amount, the stolen files could remain locked or be deleted by the cybercriminal.

Rootkit

A type of malware that opens a permanent “back door” into a computer system. Once installed, a rootkit will allow additional viruses to infect a computer as various hackers find the vulnerable computer exposed and compromise it.

Spyware

A type of malware that quietly gathers a user’s sensitive information (including browsing and computing habits) and reports it to unauthorized third parties.

Trojan

A type of malware that disguises itself as a normal file to trick a user into downloading it in order to gain unauthorized access to a computer.

Virus

A program that spreads by first infecting files or the system areas of a computer or network router's hard drive and then making copies of itself. Some viruses are harmless, others may damage data files, and some may destroy files entirely.

Worm

A type of malware that replicates itself over and over within a computer.

Why is this Important?

Aside from the obvious!

Most Cybercrime Starts with Malware

Cybercriminals use it to access your computer or mobile device to steal your personal information like your Social Security number, passwords, credit card information, or bank account information, to commit fraud.

Once cybercriminals have your personal information, they use the data for illegal purposes, such as identity theft, credit card fraud, spamming, and spreading malware to other machines.

Don’t count on your antivirus! It’s only as good as the definitions. Newer threats may not be thwarted.

Staying Safe at Home

Keep a Clean Machine

Having the latest security software, web browser, and operating system are the best defenses against viruses, malware, and other online threats.

Keeping the software on your device up-to-date will prevent attackers from being able to take advantage of known vulnerabilities.

When in Doubt, Throw it Out

Links in emails and online posts are often the way criminals compromise your computer.

If it looks suspicious, even if you know the source, it’s best to delete it.

Think Before You Act

Be wary of communications that implores you to act immediately, offers something that sounds too good to be true, or asks for personal information.

Be concerned, as well, when communication uses fear to incite action:

“Your bank account has been breached. Log in immediately to protect your assets!”

“Your email account has been flagged for inappropriate content; enter your credentials to avoid monetary penalties.”

Make Your Passwords Long and Strong

Make your password eight characters or longer and use a mix of upper and lower case letters, numbers, and symbols.

Symbols and numbers help protect against “dictionary attacks,” where an attacker tries a list of common words to guess your password.

Amount of Time to Crack Passwords

"abcdefg" 7 characters	.29 milliseconds
"abcdefgh" 8 characters	5 hours
"abcdefghi" 9 characters	5 days
"abcdefghij" 10 characters	4 months
"abcdefghijk" 11 characters	1 decade
"abcdefghijkl" 12 characters	2 centuries

Use Stronger Authentication

Always opt to enable stronger authentication when available, especially for accounts with sensitive information including your email or bank accounts.

A stronger authentication helps verify a user has authorized access to an online account.

For example, it could be a one-time PIN texted to a mobile device, providing an added layer of security beyond the password and username.

Visit www.lockdownyourlogin.com for more information on stronger authentication.

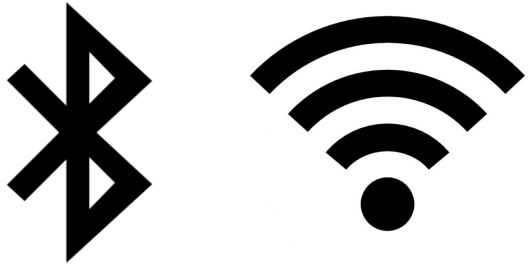
Back Up Your System

By regularly backing up your important files, you minimize the risk of a complete system failure caused by malware.

Going Mobile

Safety Away from Home

Stop Auto Connecting



Disable remote connectivity and Bluetooth.

Some devices will automatically seek and connect to available wireless networks.

Bluetooth enables your device to connect wirelessly with other devices, such as headphones or automobile infotainment systems.

Disable these features so that you only connect to wireless and Bluetooth networks when you want to.

Think Before You Connect

Before you connect to any public wireless hotspot – like on an airplane or in an airport, hotel, train/bus station or café – be sure to confirm the name of the network and exact login procedures with appropriate staff to ensure that the network is legitimate.

Do not conduct sensitive activities, such as online shopping, banking, or sensitive work, using a public wireless network.

Only use sites that begin with “https://” when online shopping or banking.

Using your mobile network connection is generally more secure than using a public wireless network.

Think Before You Click

Use caution when downloading or clicking on any unknown links.

Delete emails that are suspicious or are from unknown sources.

Review and understand the details of an application before installing.

Guard Your Mobile Device

To prevent theft and unauthorized access or loss of sensitive information, never leave your mobile devices–including any USB or external storage devices–unattended in a public place.

Keep your devices secured in taxis, at airports, on airplanes, and in your hotel room.

Apple products have the ability to be wiped remotely; if you have one of these devices, enabling “Find My iPhone (or Mac, iPad)” allows this feature to be used.

For more information, visit

www.dhs.org/stopthinkconnect