REMOTE COMPUTING BEST PRACTICES

PROVIDED BY CYBERLINKASP

You are a target so be smarter than hackers

You've heard these common "safe computing best practices" before ... but did you listen? Quick review:

1. Use strong passwords, change them often, don't use the same ones you use on personal computers or mobile devices. Example: ILoveHawaii* is 12 characters, not bad but, iL0veH@wa!!* and i{><}H@wai!* are better and best. Be creative and please don't write the password down on a sticky and keep it near the computer...pretty please!

2. Don't click on links in email or pop-ups. Buttons that read Click Here, Sign Me Up, Find Out How, Act Now, etc., are links! This tip often says 'suspicious' or 'spam' or 'unsolicited' email but it's safer to just not click on links. Press the escape key (ESC, Esc, esc) at the upper left corner of your keyboard to remove a pop-up and/or report it to tech support or your IT department, especially if it won't go away.

3. Don't do personal stuff on your work computer and don't do work stuff on your personal computer. Company data can be stolen from docs that were emailed to home computers/personal smart phones to be worked on later.

They can't hack a computer that's off

Even TV/Movie hackers can't break in to a computer that's not on. Save your company's data, reputation and hard work from the bad guys by logging off and shutting down when your computer will not be in use. Bonus: saves electricity and money. Double Bonus: most of the stuff the bad guys do with a hacked computer happens during off hours—DENIED!

Never leave your computer unattended (it gets lonely)

Don't think "It won't happen to me." It could! Make every effort to keep your computer in sight and within reach. The only way to get around tip #1 is to steal the computer and then hack it. Remote laptop users are especially at risk. And, if you step away, even for a minute, make sure you log out and turn on your screen saver lock.

Channel your favorite detective and spot the signs of malicious activity

Hover your mouse over almost any link, especially in email, and in about 2 seconds you'll see some very informative details that can guide your next move. Do I continue or delete? One of the best ways to detect a scam email is to hover your mouse over the "supposed" From: address in the email. In many email applications, this will reveal the address that the message was sent from and it's often not the address visible in the From: field. Example: the email says it's from your own email address, or the company's email, or a trusted friend/colleague's email but, with your mouse cursor held over the From: address you see a different/suspicious address—DELETE!

Turn off Bluetooth networking or any communication between devices

If your internet-connected device (smart phone, watch, etc.) can communicate directly with your computer, that opens a pathway for hackers to exploit. Even if you have permission to use the device, turn off the Bluetooth connection when not in use. A recent, now infamous, hack into a casino's network was accomplished by hacking into the aquarium. The tank had a smart sensor for water temp and such. They hacked the sensor, then the sensor's controlling computer, and then they were on the casino's internal network and they stole whatever they wanted.

Don't take the bait and become a victim of Phishers

Phishers, like old-fashioned con artists, try to hook you into doing any number of things, all of which are good for them and bad for you and your company. Phishing attacks almost always involve you being lured into clicking on a link, answering a question, signing up or re-registering for something, accepting your prize or, and this is one of the trickiest cons, validating credentials for your network/bank/shopping service/etc. All of these result in a security breach and/or identity theft. With just one click, you could enable hackers to infiltrate your organization's computer network. Phishing is also the first step to most ransomware attacks.

Avoid public Wi-Fi like it was ... public

Avoid freely accessible, easily-hackable public Wi-Fi. Use your company's virtual private network (VPN) or a personal hotspot connection through your phone. Public Wi-Fi introduces significant security risk. If you absolutely need to access the internet from a public Wi-Fi location, be aware that other people have access to that network and, without a firewall between you and them, they can hack away at your computer from across the room. Interested observers with the computer skills can monitor your traffic/data as it passes through the Wi-Fi network. And, there is always the chance that people with bad intentions can peek over and see you entering usernames and passwords or private data; it's called shoulder surfing.

In the Internet-connected world, too much sharing is just not caring

Be extra careful of what you share on social media and personal websites. The simplest innocent comment or post can be all a nefarious evesdropper needs to infiltrate your personal computer and/or company's network. Consider this seemingly harmless post: "Sorry, can't meet, company is updating our computers tonight." This reveals more than you might guess. "Gotta work late!" would've been better. Another example: You post a selfie showing how excited you are for tonight. The selfie is you in front of your computer. To a hacker, it shows that you use Outlook email on a Dell laptop with Windows 10 and it has your username and password on a sticky note next to the keyboard. Oops!

Take advantage of tech support but make sure it's really tech support

Beware of computer/tech support scams. You might receive an email or pop-up alert from someone claiming to be from your IT department or tech support. (See Tip #5) Their goal is to trick you into installing malware on your computer or mobile device, or provide them with sensitive data. What to do? Don't provide any information. Instead, contact your IT/Support department directly.

You gotta know when to hold 'em ... know when to fold 'em

Learn how to tell when something is not right on your computer. Make a conscious effort to know how long your computer takes to boot up, how long to reboot, how long to come back from sleep mode or screen saver. Make a mental note of about how long it takes to check email, save documents, log in to your company portal and shut down. The more aware you are of how your computer feels when things are working correctly, the more obvious it will be when things are just not right. Any significant change can be a red flag.