ABACODE

TOP 10 SOCIAL DISTANCING CYBERSECURITY TIPS | EMPLOYEES

1 STAY HOME!

Stay home! Not just for your physical safety, but your device as well! Social distancing can make us all a little stir crazy and going to work at the one coffee shop still open with free Wi-Fi can sound like a great idea, but these places are hot spots for hackers using the same network to attack your systems.

2 VPN

Connect to the company's VPN. If your company uses a VPN, make sure you have it connected at all times! This allows them to monitor your system to keep it safe from attackers as well as encrypting any traffic going through your systems and giving you a secure network to work in.

3 SEE SOMETHING, SAY SOMETHING

If you see something, say something. We often get a strange feeling when something "off" happens. If you see your device acting strangely, or receive a suspicious email, call a known, trusted number to verify! Make sure not to ask the suspicious email sender for a phone number, hackers have no problem answering your questions impersonating someone else.

4 NO LOCAL STORAGE

Don't use local storage if you can avoid it. Always follow your company's policy, but it's often best practice to store things in a secure data center or cloud environment. Make sure important files aren't kept on your desktop in case your computer becomes a target.

5 SECURE PASSWORDS

Make sure all your passwords are secure! And by passwords, we mean passphrases. Multiple random words that a hacker couldn't guess or successfully crack without years of trying. All your accounts should have different passphrases, and while they can be tough to remember DON'T write them on a sticky note or a Word file on your desktop! If your company uses one, make sure you fully utilize a secure password manager!

6 MULTI-FACTOR AUTHENTICATION

Enable multi-factor to everything! If your password does get compromised adding an authentication app or phone number can stop a hacker altogether, or at the very least make attacking you a much bigger headache.

7 DON'T TALK TO STRANGERS

Be wary of emails from unknown sources! If you don't recognize the sender of an email there's a chance it's an attacker reaching out to you. Phishing emails are the top way for an attacker to breach into systems, and being aware of this can help you act appropriately.

8 DON'T KNOW, DON'T DOWNLOAD

Don't download unknown files or attachments! Something simple as a PDF file can give a hacker full access to your computer, all its files, its webcam and microphone, everything just by opening it! If you don't know the sender or trust the source of any file don't download it or open it on your computer!

9 UP TO DATE

Make sure your programs are up to date! This includes your operating system like Windows and Mac OS, web browsers like Google Chrome and Mozilla Firefox, and of course your antivirus! This won't stop all attacks but managing your vulnerabilities can make you a much trickier target

10 LOCK IT UP

Lock your computer when you're away. This can prevent other people around the house such as young children from getting curious and using your work computer for personal browsing. This is easy to do with a keyboard shortcut! On Windows press the Windows key and 'L' together, on Mac it's Control-Shift-Power.

BONUS TIP!

If you can log into your local router see if you can create your own separate work network. This is often easy to do with a few clicks and setting a secure password to make sure the other devices in your home don't pose a security risk to your work computer!