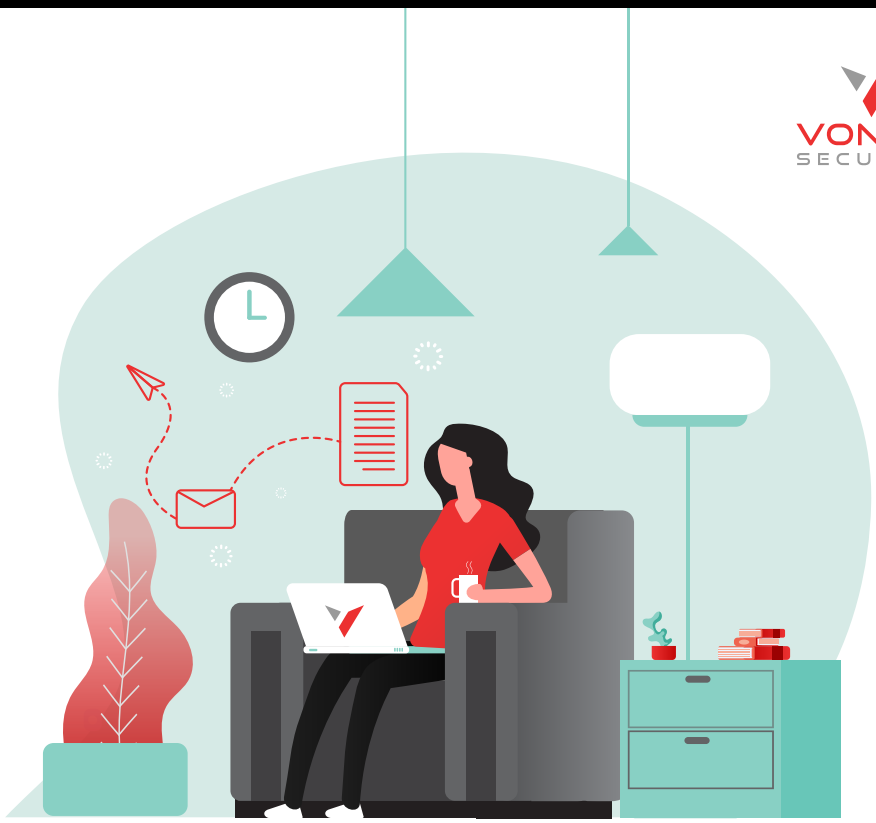
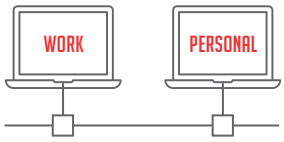
10 CYBERSECURITY SURVIVAL TIPS FOR WORKING REMOTELY

VONAHI SECURITY



1 Use two-factor authentication

Two-factor combats phishing attacks that attempt to steal your credentials. Authentication attempts will require a code that only you can retrieve.



2 Use two separate machines

Do work on your work computer and personal computing on your personal computer. If you intermix the two, you increase the chance that an infection will contaminate both your work and personal life.

3 Harden Wi-Fi access points

Ensure any wireless access points on your network are appropriately hardened. As an added layer of protection, turn off Wi-Fi broadcasting so that you must know your SSID to connect to it, that way only those who know your SSID can connect to you.

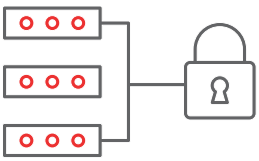
4 Avoid public Wi-Fi when possible

(delete saved networks such as Starbucks, Delta Wifi, Gogoinair, airport wifis, etc.)

Be careful using public Wi-Fi if you're working on the go. Public Wi-Fi tends to have lax or nonexistent security—leaving the network and your mobile devices vulnerable to hackers.

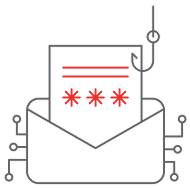
5 Keep systems up-to-date (both personal and work)

Installing system and software updates is the best defense against common viruses and malware online, especially Windows. By downloading and installing the updates, you patch the vulnerabilities that virus writers rely on to infect your computer.



6 Use password managers where possible

Don't use the same password for everything. If an attacker gets one password, then they get them all. A password manager ensures that you have unique and strong passwords for all of your accounts and can make remembering all of the passwords far easier.



7 Beware of phishing emails

(especially those related to coronavirus and corporate emails)

Cybercriminals are increasingly trying to take advantage of the ongoing pandemic by playing into people's fears via Covid-19 themed phishing campaigns, cyber scams and malware campaigns. Be alert.

8 Verify any and all phone calls and emails from IT

(Ask them to confirm your employee ID)

If you're suspicious, inform your caller you'll give them a call back. When dialing back, use the number your organization has provided for their IT department. If your organization uses an internal wiki or code of the day, request this from them.

9 Never share your password, even with "IT"

(as they can usually reset it if needed)

Your IT department should never ask you for a password, especially since they can reset it at any given moment. If someone is asking for your password, that call should be treated as highly suspicious and perhaps reported to your IT department.

10 Double down on skepticism

You've got to turn your risk detector on HIGH when working remotely. If you've got any doubt about a message in your inbox when you're on your phone, defer acting on that message until you can look more closely.