Quiz

How secure is your workstation?

1 Who manages your computer, laptop or workstation?

(A) My IT department.

(B) A local IT provider.

(C) Each employee is responsible for their own device.

2 How often do you save your work to a second location?

(A) Our IT team automatically backs up files once a day.

(B) A few times a month (I hope.)

(C) I don't save my files to a second location.

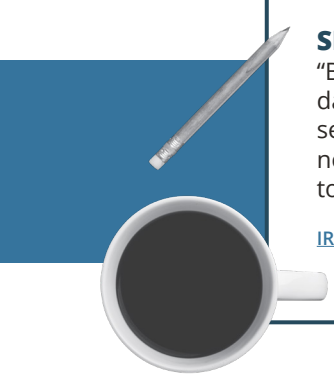
SECURITY TIP: "Backups will let you restore your data in case a computer breaks, an employee makes a mistake, or a malicious program infects your system. Without data backups, you may have to recreate your business information manually (e.g. from paper records)." NIST, US Department of Commerce

3 How does your IT team monitor for unusual system activity?

(A) With an intrusion detection system.

(B) I know activity is monitored, but I don't know how.

(C) We don't monitor for unusual activity.



SECURITY TIP: "Back up sensitive data to a safe and secure external source not connected fulltime to a network."

IRS Publication 5293

4 It's 6 PM on a Friday night and you are facing a tight deadline when your computer suddenly goes dark. When you finally get it working again, you realize the files from this morning are totally missing. What do you do?

(A) Call my technical support team immediately to see if they can help.

(B) Call my technical support team on Monday to see if they can help.

(C) Accept the fact that I'll be pulling all-nighters this weekend to catch up on the work I just lost.

5 You receive an email from a name you (think you) recognize. After opening the attachment, you realize it's malware…and all computer files are now inaccessible. How do you react?

(A) My IT team stores daily backups of my work, and the files on my computer are encrypted, so I'm not too concerned.

(B) Hope that my IT team has recent file backups, then start preparing "Your Data May Be Compromised" notifications for customers.

(C) I have no idea.

SECURITY TIP: "Drive encryption, or disk encryption, transforms data on the computer into unreadable files for the unauthorized person accessing the computer." IRS.gov

SECURITY TIP: "Antivirus software scans files or computer's memory for certain patterns that may indicate the presence of malicious software (i.e., malware). Antivirus software (sometimes more broadly referred to as anti-malware software) looks for patterns based on the signatures or definitions of known malware." IRS.gov

6 What kind of antivirus software does your company use?

(A) Our internal or external IT support team manages our antivirus software.

(B) We all use something (like Norton or McAfee) but it's not standard.

(C) Whatever came pre-installed on my computer.

7 Which best describes your company's security policy?

(A) Thorough, advanced and readily available.

(B) Boxed, simple and talked about during onboarding.

(C) Nonexistent.

SECURITY TIP: "Establish basic security practices and policies for employees, such as requiring strong passwords and appropriate Internet use guidelines, that detail penalties for violating company cybersecurity policies." FCC.gov

8 Which best describes your company's remote work policy?

(A) Strict.

(B) Optional.

(C) What remote policy?

9 How often are security patches issued to your company's network-connected devices?

(A) As soon as they become available.

(B) Whenever our IT team has the time (I think.)

(C) I don't know.

SECURITY TIP: "Many companies and organizations have a VPN. VPNs allow employees to connect securely to their network when away from the office. VPNs encrypt connections at the sending and receiving ends and keep out traffic that is not properly encrypted. If a VPN is available to you, make sure you log onto it any time you need to use a public wireless access point." CISA.gov

10 I use a VPN (Virtual Private Network) to connect to company resources.

(A) True.

(B) False.

(C) I don't know.

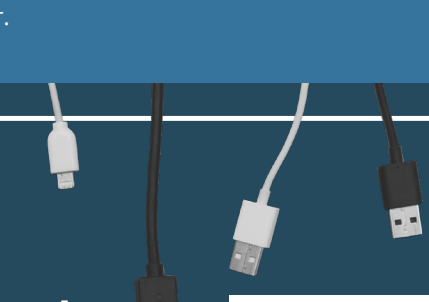
11 How often does your company teach you about cyber threats?

(A) At least once a year.

(B) During onboarding, but not since.

(C) I can't remember.

SECURITY TIP: "Training should focus on threats employees encounter, like phishing emails, suspicious events to watch for, and simple best practices individual employees can adopt to reduce risk. Each aware employee strengthens your network against attack, and is another 'sensor' to identify an attack." CISA.gov



Learn more about Right Networks Secure Workstation

Contact your Account Executive to learn more, or:

If you work for an accounting firm, call **888.245.0292**.

If you work for another type of business, call **888.245.0295**.

Right Networks®

You answered...

MOSTLY As: Your company may be aware of the latest cyber threats—but how sure are you about those answers above, anyway? It's better to be safe than sorry. Contact your IT support team immediately to discuss your security policies, especially if those policies have not been updated in the last year.

MOSTLY Bs: You may be doing some things right when it comes to protecting your computer—but because security protocols are unclear, your data is still at risk. Contact your IT provider for a thorough review of their backup schedule, storage and encryption procedures, and all other best practices recommended by the FCC, ASAP.

MOSTLY Cs: Don't wait until tomorrow. Don't even wait until after lunch. Contact Right Networks to learn how Secure Workstation helps protect you and your company's data, immediately.