

THE SHORTEST END-USER CYBERSECURITY TRAINING OF ALL TIME!

We know that you're busy: focus on the below tips to instantly improve the cybersecurity of your business.



1



Use Strong, Unique Passwords:

Each account should have a different password, ideally generated by a password manager, and changed regularly.

2



Enable Multi-Factor Authentication:

Always opt for MFA where available to add an extra layer of security beyond just a password.

3



Recognize and Report Phishing:

Learn the signs of phishing emails—such as urgent requests for information, unexpected attachments, or unfamiliar sender addresses—and report them immediately.

4



Be Wary of Unsolicited Phone Calls:

Don't provide any personal or company information over the phone unless you've verified the caller's identity and legitimacy.

5



Use Secure Wi-Fi Networks:

Avoid unsecured public Wi-Fi for work-related activities. If you must, use a reputable VPN to encrypt your connection.

6



Don't Plug in Unknown USB Drives:

They could be infected with malware. Only use company-approved storage devices.

7



Secure Your Workstation:

Lock your screen whenever you step away, even for a moment.

8



Be Careful with Social Media:

Think before you post, particularly when it comes to potentially sensitive information about yourself or the company.

9



Avoid Suspicious Downloads:

Don't download files or applications from untrusted sources, and stay away from suspicious websites.

10



Follow Company Policies:

Adhere to your company's IT security policies and guidelines, and stay informed about new procedures.