

Cyber Safety Basics for Your Team

Technology can block a lot, but a well-crafted scam still lands in someone's inbox. This guide is written for everyone on your team, not just IT. Print it, share it at a staff meeting, or add it to new-hire onboarding.

For everyone on the team. Keep this guide handy and share it with new hires.

1 Spotting a phishing email

- ☐ **Check the actual sender address, not just the display name**
'Your CEO' can be anyone@anywhere.com.
- ☐ **Be suspicious of urgency, secrecy, or pressure**
'Need this in the next 10 minutes, don't tell anyone' is a classic warning sign.
- ☐ **Hover over links before you click**
If the address doesn't match what you expect, don't click.
- ☐ **Don't open attachments you weren't expecting**
Even from people you know. Their account may be compromised.
- ☐ **When in doubt, report it**
Use your Report button or forward it to IT. Reporting a real email is never a problem.

2 Money & sensitive requests

- ☐ **Verify any change to bank or payment details by phone**
Call a number you already have on file, never the one in the email.
- ☐ **Never buy gift cards because an email or text asked you to**
No real manager or vendor asks for payment this way.
- ☐ **Never approve an MFA prompt you didn't start**
If your phone asks you to approve a sign-in you didn't make, deny it and tell IT.

3 Passwords

- ☐ **Use a long passphrase instead of a short, complex password**
Four or more random words is stronger and easier to remember.
- ☐ **Use a different password for every account**
One leaked password shouldn't unlock everything.
- ☐ **Let the password manager do the remembering**
Never share passwords by email, text, or chat.

4 Devices & AI tools

- ☐ **Lock your screen whenever you step away**
Windows key + L on a PC, Control + Command + Q on a Mac.
- ☐ **Restart when updates are waiting**
Delaying updates leaves known holes open.
- ☐ **Don't plug in USB drives you found or didn't expect**
Hand them to IT.
- ☐ **Avoid public Wi-Fi for work unless you're on the company VPN**
A phone hotspot is a safer choice.
- ☐ **Don't paste client or confidential data into unapproved AI tools**
Use only the AI tools your company has approved.

5 If something goes wrong

- ☐ **Report it immediately, even if you're embarrassed**
Minutes matter. Nobody gets in trouble for reporting quickly.
- ☐ **If you see a ransom message or files being renamed, disconnect from the network**
Unplug the cable or turn off Wi-Fi, but don't power the computer off.
- ☐ **Don't try to fix it yourself or delete evidence**
Let IT investigate.

Want training that sticks?

FUSION 1 offers interactive security awareness training and phishing simulations for small teams.

[Book a free IT review](#)

Call or text 814-499-2119
Toll-free 888-279-9776

This checklist is general guidance for small businesses and is not legal, compliance, or insurance advice. © 2026 FUSION 1 IT Solutions. You're welcome to share this document unchanged.