PREVENTING CYBERCRIME AT WORK

YOU'VE RECEIVED A PHONE CALL OR MESSAGE...

REMAIN SILENT, AVOID CLICKING ANYTHING, AND ASK YOURSELF THESE QUESTIONS.

- Is the message or call **unexpected**?
- Is the tone **urgent**, alarming, accusatory, or overly congratulatory?
- Are you being asked for **personal information**?
- Are you being addressed as **Sir or Madam**?
- Is the text or email full of **grammatical errors**?

"YES" TO ONE OR MORE

"NO" TO ALL

SEEMS SAFE. PROCEED WITH CAUTION.

HAVE YOU OPENED ANY SUSPICIOUS CONTENT OR SHARED PERSONAL DETAILS?

NO

1. Remain **silent and avoid responding** to the caller or sender.
2. **Do not provide any personal details** (name, payment info, organization, address, birthdate, business affiliations, or peers/family info).

YES

- ☑ **Do not click on or open** anything else.
- ☑ **Disconnect from Wi-Fi or cellular data** on your device if you opened content.
- ☑ **Shut down your device** to stall malware if you opened content.
- ☑ **Lock your credit card and place a hold on your bank account** through a separate device if you gave the scammer your financial information.
- ☑ **Reset any passwords** for all important accounts on a separate device.
- ☑ **Inform your manager** about the issue.
- ☑ **Contact an IT professional** for help.

WHAT TYPE OF COMMUNICATION DID YOU RECEIVE?

PHONE CALL

1. Continue to **respond as little as possible.**
2. Ask questions about the caller's **intentions** if you are still uncertain of the call's legitimacy.
3. **Decline and hang up** if the caller asks for personal details.

__Note:__ Legitimate companies post notifications on your personal account, send you an official document, or send you a mailed invoice.

THINK IT WAS A SCAM?

YES

EMAIL

DOES THE SENDER'S EMAIL ADDRESS HAVE ANY OF THESE TRAITS?

Random letters and numbers:

PayPal <paypal@fidgacporej2654.com>

OR

Domains like @gmail or @yahoo paired with legitimate names:

PayPal <paypal@gmail.com>

OR

Random capitalizations or misspelled company names:

PayPal <paypal@PaypalL.com>

OR

Display names with email addresses instead of company names or first/last names:

paypal@mail.paypal.com <paypal@kjbl1358edjfik.com>

YES

NO

IS THERE A FILE ATTACHMENT WITH AN EXTENSION LIKE THESE?

.ade, .adp, .asf, .bas, .bat, .chm, .cmd, .com, .cpl, .crt, .dll, .exe, .hlp, .hta, .htm, .html, .inf, .ins, .isp, .jar, .js, .jse, .lnk, .mdb, .mde, .mov, .msc, .msi, .msp, .mst, .pcd, .pif, .psc1, .reg, .scf, .scr, .sct, .shs, .swf, .url, .vb, .vbs, .vbe, .vbs, .wsc, .wsf, .wsh

(These can modify or erase your hard drive.)

OR

.gif.exe, .jpg.htm, .mpg.bat

(Double extensions)

YES

TEXT MESSAGE

IS THE PHONE NUMBER UNUSUALLY LONG?

***Note:** Legitimate marketing texts only use 6 digits or a 10-digit toll-free number.*

NO

IS THE SUBJECT OF THE TEXT PART OF A TEXT SCAM? (GOOGLE IT!)

YES

NO

SEEMS SAFE. PROCEED WITH CAUTION.

BLOCK THE NUMBER AND/OR DELETE THE EMAIL OR MESSAGE THREAD.

How do cybercriminals target you?

- **EMOTIONAL MANIPULATION:** Fraudulent communication often contains messages that increase your fear, guilt, or excitement. Heightened emotions can distract you and make you more susceptible to scams and phishing.
- **THE FACADE OF SAFETY:** Other types of fraud can seem innocuous, meaning you'll be more likely to open a link or attachment or even provide personal details.
- **POSING AS A TRUSTED SOURCE:** Scams can pose as a business or friend, and their associated instructions may ask you to provide personal details or log in using your password.
- **MALWARE:** If you open a link or attachment, it may install malware onto your hard drive. Malware can take the form of a virus that spams your contacts or ransomware that locks your files until you pay money.

LEARN MORE ABOUT CYBERCRIME PREVENTION

SCAN ME