OCTOBER CAMPAIGN

Cybersecurity Awareness Month

A Practical Safety Guide for Families & Parents

Protecting your family online starts with simple everyday habits! Digital safety doesn't have to be complex. Use this quick guide to keep your household safe from digital scams when checking emails and clicking web links.

Smart Email Habits

- **Inspect the Sender Address:** Display names can be easily fake. Always check the full email address behind the name to confirm who sent it.
- **Watch for Fake Urgency:** Scammers create artificial panic (e.g., *"Account locked in 24 hrs!"*). Take a breath and verify independently.
- **Beware of Unexpected Attachments:** Avoid opening unexpected files, invoices, or zip folders—especially from unknown sources.
- **Keep Private Details Private:** Banks, schools, and legitimate organizations will **never** ask for passwords or SSNs via email.

Safe Link Practices

- **Hover Before Clicking:** Hover your mouse cursor over any link to preview the actual destination URL at the bottom of your screen.
- **Check Domain Spelling:** Look closely for subtle typos or fake extensions (like `paypal-security-update.com` instead of `paypal.com`).
- **Look for Secure Connection:** Ensure web addresses start with `https://` when entering personal or financial information.
- **Go Straight to the Source:** When in doubt, open a new browser tab and manually type the official website address yourself.

3 Golden Rules for Every Family Member

1

When in doubt, throw it out

If a message or email feels strange or too good to be true, trust your instincts and delete it.

2

Use Passphrases

Combine 3-4 random words, numbers, and special symbols, or use a trusted password manager.

3

Turn On 2FA

Enable Two-Factor Authentication across all key family accounts for an extra wall of defense.

LOCK ACCOUNTS · INSPECT LINKS · UPDATE SOFTWARE · TALK WITH KIDS