CYBERSECURITY MATTERS

PRACTICE THESE ESSENTIALS TO STAY SAFER ONLINE

Phishing Awareness Tips

Hover Before You Click:
Always hover over links before clicking — if the real URL looks off or doesn't match the sender, skip it.

Watch for Lookalike Sites:
Scammers love sneaky typos. Check for swapped letters or numbers (like "paypa1.com") before you trust a site.

Think Before You Act:
If an email feels odd or asks for something unusual, take a second look — it might not be legit.

Beware the Rush:
"Act now!" "Your account will close!" Urgent language is a classic phishing trick to make you click fast.

Verify the Sender:
Just because it looks like it's from someone you know doesn't mean it is. Confirm through a known contact method.

Don't Move to Text:
If someone tries to take the convo off email, it's a red flag. Scammers often switch to text to dodge filters.

Using the Phish Alert Button

See Something Suspicious? Report It!:
If an email feels phishy, hit the Phish Alert button instead of deleting it — IT will investigate.

Your Report Protects Everyone:
Reporting one bad email can help stop campus-wide scams. Every alert makes a difference!

Don't Forward, Just Report:
Never forward suspicious messages — use the button to safely send it straight to the security team.

Password Best Practices

Update Regularly:
Change your password every few months to keep your accounts secure — especially after a breach notice.

Avoid Reuse:
Never recycle old passwords or use the same one across multiple accounts. One leak can expose them all.

Build a Strong One:
Use a mix of words, numbers, and symbols — or better yet, a passphrase that's long and memorable.

BUILDING A CYBER STRONG AMERICA

CYBERSECURITY AWARENESS MONTH
OCTOBER 2025

cisa.gov/cybersecurity-awareness-month