



October is Cybersecurity Awareness Month

*Stay Safe. Stay Smart.
Stay Secure Online.*



Cybercrime is on the rise, and scammers are smarter than ever. But protecting yourself online doesn't have to be complicated. Small steps make a big difference.



Watch for AI-Enhanced Phishing Emails

Cybercriminals now use AI to craft emails that look real—very real.

- Be skeptical of unexpected attachments
- Hover over links before clicking
- Verify payments or bank changes by phone



Strengthen Password Hygiene

- Weak passwords = open door for attackers.
- Use a password manager
- Create long passphrases (e.g. GreenTractor!CoffeeSky92)
- Never reuse passwords across login



Stay Alert on Public Wi-Fi

Hackers love airports, hotels & coffee shops.

- Use a VPN
- Turn off auto-connect
- Avoid accessing sensitive accounts on public networks



Common Online Scams - 2025

- Fake package delivery texts
- "Your account is locked" emails
- Romance scams
- Fake tech support pop-ups
- Social media giveaway scams
- AI Voice Scams (Deepfake Family Emergencies)
- Banking Text Scams (Smishing)
- Facebook Marketplace / Online Selling Scams
- Student Loan Forgiveness Scams
- Crypto Investment Scams
- Job Offer Scams

You Can Stay Safe Online

A few simple habits protect your identity, your money, and your privacy.

- Think before you click
- Protect your accounts
- Keep software updated
- Ask for help if you're unsure

Watch Out for Scams

Scammers are using AI to make messages look real.

- Don't click on links from unknown senders
- Look closely at email addresses
- If something feels urgent or threatening—pause and verify
- If something seems too good to be true—it is.