Avast

Quick Guide to Better Online Safety

Cyber Safety Checklist

Practice good cyber habits with this checklist:

Safer Posting and Sharing

- ☐ Don't share, post or email your personal information on social media
- ☐ Don't forward suspicious emails or links to friends and family

Safer Browsing

- ☐ Create strong passwords with easy to remember phrases, numbers and characters
- ☐ Vary your passwords across your websites and accounts
- ☐ Install and regularly update antivirus programs

Safer Downloading

- ☐ Only download material from reliable sources
- ☐ Avoid opening attachments or clicking on links from unknown senders

Safer Banking

- ☐ Monitor your bank and credit card statements for unusual charges
- ☐ Shred personal information and financial statements before throwing them away
- ☐ Visit the official website of your bank or charity when making an online payment or donation

Potential Scam?

Look for these five red flags:

- **Time pressure:** Are they rushing you to make a decision or payment quickly?
- **Unfamiliar contact:** Don't open a message or attachment from an unknown source or number
- **Strange domains or links:** Despite coming from a familiar name, beware of sources that are misspelled or don't match the sender's email address
- **"Free" prizes or giveaways:** These emails may contain malware or attempt to steal your information
- **Unsolicited updates:** Beware of any requests to update or confirm your personal information

Take these steps if you think you're being scammed:

1. Cease communication with the potential scammer
2. Close your computer or device
3. Call someone you trust
4. Call the National Elder Fraud Hotline at **833–FRAUD–11**

#BeCyberSmart