THINK BEFORE YOU CLICK

Small actions. Big protection.



GUARD AGAINST IDENTITY THEFT

Check your accounts regularly for suspicious activity.

Be alert for:

- ✓ Transactions you don't recognize
- ✓ Unexpected account alerts
- ✓ Bills for accounts you didn't open
- ✓ Credit inquiries you weren't expecting
- ✓ If something doesn't look right, contact your credit union immediately.

SPOT THE SCAM

Phishing emails and text messages often try to create urgency or curiosity.

Watch for:

- ✓ Unexpected emails or texts asking you to act immediately
- ✓ Requests for passwords, account numbers, or verification codes
- ✓ Links or attachments from unfamiliar senders
  Messages that seem "too good to be true"

When in doubt, don't click. Contact the company directly using a trusted phone number or website.

PROTECT YOUR ACCOUNTS

- ✓ Use a unique password for every account
- ✓ Turn on Multi-Factor Authentication (MFA)
- ✓ Keep your devices updated
- ✓ Use a password manager

SHOP ONLINE SAFELY

- ✓ Shop only with trusted retailers
- ✓ Look for https:// before entering payment
- ✓ Avoid making purchases on public Wi-Fi
- ✓ Be cautious of unbelievable deals
- ✓ Verify QR codes before scanning

THINK BEFORE YOU CLICK

Before clicking a link, opening an attachment, scanning a QR code, or responding to an unexpected message, ask yourself:

- ✓ Was I expecting this?
- ✓ Do I know who sent it?
- ✓ Does this seem legitimate?