How To Stay Cyber Safe During Phishing Season

Only shop on popular or familiar websites

Make sure websites aren't fake - especially those sent via email or text!

Beware of misspellings or sites using .io instead of .com.

Don't click on spammy ads.

Omit personal information on shopping forms

Only include information such as payment method and mailing address.

When in doubt, look for the lock

Make sure there is a lock icon near your browser's address bar.

Never buy anything from a site that doesn't display this - your data transfers are far more secure under SSL than an unencrypted site!

Use a credit card for online payments

Only use a credit card or mobile payment app to shop. The Fair Credit Billing Act ensures you are only responsible for up to $50.

Using Apple Pay or Google in store allows you to avoid card skimmers.

Next Steps: If you think you are scammed

If you think something is wrong with your credit, debit, or checking account statements, alert your financial institution and the Office of Consumer Protection.

Freeze your credit across all three main credit bureaus (Experian, Transunion, & Equifax).