CARPATHIA CREDIT UNION КАРПАТІЯ

Protect Yourself On and Offline

How to Avoid Becoming the Target of a Phishing Scam

Phishing scams are modern day scams where a malicious user or entity will mimic a trusted organization's identity to gain information or access to personal accounts and data.

As of July 31, 2020, the impact of fraud this year alone has totaled $54 million with almost 15,000 people falling victim to it.

These scams exist in numerous forms: emails, phone calls, and fake websites and login portals, among others.

There are some simple steps you can follow to reduce the chances you will be targeted by a phishing scam when doing online banking – a common place for phishing emails, fake websites and login portals:

- Never search for your credit union website on a search engine when looking to do online banking. Always type in the credit union's actual URL and then navigate to online banking.
- Once at the right website, navigate to the login page and look for these clues to verify that you are on the credit union's actual, secure online banking site:
- All credit union websites use Hypertext transfer protocol secure (HTTPS), which means their links all start with HTTPS. If your login page link starts with HTTP, then you may be using a spoof site.
- If you see any typos on the website you are using to login to your online banking, this is a very strong indicator it is a faked page.
- Most secure login sites show a small padlock next to the link. This indicates you are visiting the website using a secure connection.
- Browse around the site before entering any information to ensure it actually has more pages than just the login or home page, and check the other pages for typos or any other unusual elements.
- Once you've verified you're on the correct secure site, bookmark it. That way, when you use the bookmark in the future, whenever you go to sign in to online banking, you will know you are on the credit union's secure site.
- Before logging in, especially on a mobile device, be sure to close any other downloaded apps that may be running in the background.
- Never login to your online banking from an email. If asked to view your account, open online banking in a separate window and use your bookmarked link to get to the website. You can also simply type in your credit union's actual URL.
- Make sure you are online banking from a device free of malware, spyware and any viruses.