Watch Out for Phishing Scams

Top 5 ways fraudsters try to steal your information

Cybercriminals are counting on us to be distracted and let our guard down. If we do, they can trick us into handing over our personal or financial information using one of their favorite tactics – phishing.

You might be familiar with email phishing but it's not the only type of phishing you could experience. Criminals will also use phone calls, text messages, websites and social media to deploy a phishing scam.

Below are some common forms of phishing that you might encounter and the warning signs to look out for.

Phone call phishing

Warning signs to look out for

1. A phone call from **"your credit card company"** or "financial institution", typically from someone who works in the "Security and Fraud Department"
2. You are told your card has been flagged for suspicious transactions and you need to **prove that you have the card** in your possession
3. You are asked to **provide the three-digit security code** on the back of your payment card, a one-time passcode that was just sent to you, or your PIN

Email phishing

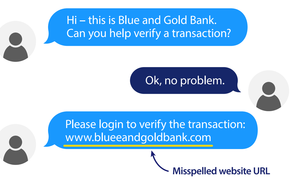
Warning signs to look out for

- Spelling and grammar **errors** in the subject line or body of the email
- **Deadline.** Sometimes scammers will include a deadline and threaten account suspension to add urgency to override your normal sense of caution
- The email address **doesn't match** the organization (i.e., irs.net or amazon.mil)
- The email does not address you by **name**
- **No contact information.** If something feels suspicious, contact your financial institution directly using the phone number on the back of your card
- **Suspicious hyperlinks.** Avoid clicking on hyperlinks if possible. A single click can cause your computer to become infected with malware

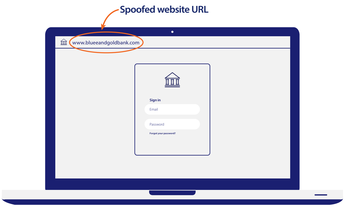
Text message phishing

Warning signs to look out for

- There's a **link** instead of a phone number to call
- The text you receive may not contain the **name of the bank** or any other information
- The text requests that you **log in** to your bank account to verify a transaction, enter your PIN, or provide your 3-digit CVV code



Website phishing



Warning signs to look out for

- There's something **slightly off** about the web address or the actual page. Look for misspelled words, substitutions or updated logos
- An **unusual pop-up** on the site that requests that you enter your account information
- There are **HTML links** that don't match their destination

Social Media Phishing

Warning signs to look out for

- A friend request from someone you don't know
- A post asking you to click on a link that requests personal information

Have you encountered a phishing scam?

For more information on phishing and other computer-based scams, visit the National Cyber Security Alliance at **https://staysafeonline.org/**