Protect Your Online Accounts from Phishing

Keep your accounts out of the wrong hands

Phishing is an all-too-common way for scammers to learn your personal information and access your financial accounts. To help prevent yourself from falling victim to a scam, it's wise to learn exactly how phishing works.

What is phishing

Phishing is a type of social engineering technique that aims to trick you into sharing information, such as your password or account number, according to Bankrate.com. Rather than hacking into your computer, social engineering works by gaining your trust and manipulating you. With phishing, in particular, a scammer may pose as your friend or a company sending you a text message or an email.

According to the Federal Trade Commission, the message or email will relay a story to convince you to click on an attachment or link. They may say you have an issue with your accounts, you need to confirm confidential information, or you need to make a payment. If you click on the attachment or link, Bankrate.com says that malware may install onto your computer or you may be prompted to enter your username and password on a page that is similar to an online financial site or company's login page. With this information, a hacker can then access your account and steal your information or money.

How to spot a phishing scam

Phishing purposefully disguises messages to look like they are from a trusted source, making it difficult to tell that they are scams. However, there are many clues that indicate when an email is not actually from your financial partners. Alison L. Deutsch, writing for Investopedia, says that a phishing email may have grammatical errors that a legitimate email would not have.

Phishing emails may also link to sites with URLs like are either completely different or slightly altered from the URLs of a company's sites, according to Bankrate.com. Before clicking a link, hover your mouse over it, and check that the URL exactly matches the URL of the real site. Even better, Deutsch says not to click any link in an email that asks for your personal information. A reputable site will not ask for your password through an email or text message. If you are concerned about the content of an email, you can call the institution or business directly or log in to your account using a website that you know is real.

What to do after being scammed

If you believe you may have fallen victim to phishing, there is still hope that the scammer has not been able to access your account. According to the FTC, multi-factor authentication, which requires at least two different credentials to access your account, can help protect against phishing. For example, if you only give your password to a

scammer, but your account requires both a password and a face scan to log in, they may not be able to log in.

Whether or not you have multi-factor authentication, Justin Pritchard, writing for The Balance, recommends calling your financial institution if you believe you gave your credit card number or account information to a scammer. Furthermore, Deutsch says to delete any software you downloaded from an email and to immediately change your passwords. By acting fast, you may be able to change your password before a scammer even attempts to log in to your account.

Hopefully, by more cautiously reading emails and knowing the signs of phishing, you can avoid these scams.