Beware of Phishing Scams: Don't Take the Bait

Identity thieves like to go "phishing" — pronounced "fishing" — on the Internet for consumers' personal financial information using fake emails and websites to trick people into providing Social Security numbers, bank account numbers and other valuable details.

Typically, the most common phishing emails pretend to be from a bank, a retail store or government agency to lure you into divulging personal financial information, and often use a variety of tricks to make the email look legitimate. They might include a graphic copied from a bank's website or a link that looks like it goes to a bank's site, but actually leads to a fake site.

Also beware of "pharming." In this version of online identity theft, a hacker hijacks Internet traffic so when you type in the address of a legitimate website you're taken to a fake site. If you enter personal information at the phony site, it is harvested and used to commit fraud or sold to other identity thieves.

Here are some tips to avoid becoming a victim of a phishing or pharming scam.

Be suspicious if someone contacts you unexpectedly online and asks for your personal information. *It doesn't matter how legitimate the email or website may look. Only open emails that look like they are from people or organizations you know, and even then, be cautious if they look questionable.*

For example, scam artists may hack into someone's email account and send out fake emails to friends and relatives, perhaps claiming that the real account owner is stranded abroad and might need your credit card information to return home.

Be especially wary of emails or websites that have typos or other obvious mistakes. "Because some requests come from people who primarily speak another language, they often contain poor grammar or spelling," said Amber Holmes, a financial crimes information specialist with the FDIC.

Remember that no financial institution will email you and ask you to put sensitive information such as account numbers and PINs in your response. *In fact, most institutions publicize that they will never ask for customer personal information over the phone or in an email because they already have it.*

Assume that a request for information from a bank where you've never opened an account is probably a scam. *Don't follow the link and enter your personal information.*

Verify the validity of a suspicious-looking email or a pop-up box before providing personal information. *Criminals can create emails stating that "you're a fraud victim" or a pop-up box with another urgent-sounding message to trick people into providing information or installing malware (malicious software). If you want to check something out, independently contact the supposed source (perhaps a bank or organization) by using an email address or telephone number that you know is valid.*