CFA Consumer Federation of America

Slam the Door on Phishing Scams

“Phishing” is a funny-sounding word for a very serious problem. It’s when crooks contact you pretending to be from well-known companies, organizations, or government agencies and try to trick you into giving them your Social Security number, financial account information, passwords, or other personal information. They may use that information to make unauthorized purchases, use your accounts, open new accounts in your name, or even apply for a job or get tax refunds and other government benefits.

If someone suddenly appeared at your door asking for your personal information, you’d be suspicious – and rightfully so. It should be no different when someone approaches you through your computer or by phone asking for that information. These tips will help you recognize phishing scams and avoid becoming a victim.

- **If anyone contacts you unexpectedly requesting your personal information, ask yourself “why?”** If it’s a company that you have an account with, an organization that you belong to, or someone else that you have a relationship with, wouldn’t they already have that information? And if it’s not, what business is it of theirs?

- **Don’t fall for scare tactics.** These crooks will often try to push you into acting immediately, before you have time to think or check out their stories. They may threaten that your account will be suspended or that something else bad will happen if you don’t give them your information right away. That’s a tell-tale sign of fraud.

- **Look for other clues that emails might be phishing scams.** Misspellings or grammatical mistakes in emails asking for your personal information are danger signs of fraud (but if there are no mistakes, that’s no guarantee that the message is legitimate). Also, is there anything strange about receiving the message? For example, is it from a shipping company when you haven’t ordered anything? Or from a business or organization that doesn’t usually send you emails?

- **Know that phishing emails can also look like messages that you might not be surprised to receive.** The message may appear to be for a bill that you normally pay online, a notice from your bank or credit card issuer, an eCard from a friend, confirmation of an order, a request to “friend” or link to someone in a social network, or a message from your employer. If the sender’s email address is different than usual or doesn’t make sense considering who the message says it’s from, that’s another danger sign. But don’t rely on the sender’s email address to decide whether the message is legitimate, since a crook can easily mask the address to look genuine when it’s not.

- **Think before you click.** Clicking on a link in a phishing message could take you to a phony website asking for your account number, password and other personal information. Or it might download spyware into your computer or mobile device. And don't click on attachments or pictures unless you are sure of the source, since they can also carry spyware. Look up the website of whoever the message appears to be from and go to it directly. Also, don't call the phone number in the email because it may connect you to a phony office. Look the number up independently.

- **Watch out for phishing by phone.** Scammers may call you or send a text message, using the same tactics as they do in phishing emails, to try to get your personal information. And sometimes they fake their Caller ID to make it seem like they're someone they're not.

- **Be aware that some calls asking to confirm information may be legitimate.** For instance, your financial institution may call if there is an unusual purchase on your account to confirm that you made it. But it likely doesn't need to ask for your account number because it already has it. If you get a message on your voicemail that says it's from your bank or credit card issuer and asks you to call back, look up the number independently, from your statements, the phone book or online.

- **Keep your guard up.** There are many variations of phishing scams. One popular scam involves crooks claiming to be from Internet service providers or tech security companies and asking people for their passwords to fix virus problems on their computers. In another, the scammers pretend to be from the government and tell people that they need their Social Security number to sign them up for new national health care benefits. But crooks are constantly looking for new pitches to use, so new phishing scams pop up every day. They're also becoming more sophisticated. While many phishing attempts are made randomly in the hope that enough people will respond to make them profitable, some are more targeted. For instance, a scammer may look for employees' email addresses on a company's or organization's website and send those people phishing messages that appear to be from their employer.

- **Make sure your computer, laptop, notepad, and smartphone are secure.** Use antivirus and antispyware software on these devices to protect you in case you open or click on something that you shouldn't.

- **Learn more about how to recognize and avoid phishing.** Cornell University's "Phish Bowl," www.it.cornell.edu/security/safety/phisbowl.cfm, provides examples of common phishing emails. Other good sources of information include the federal government's www.onguardonline.gov website; the nonprofit National Cyber Security Alliance, www.staysafeonline.org; and the National Consumers League's Fraud Center, www.fraud.org . You can also watch the funny video about phishing and learn about other common scams by visiting Consumer Federation of America's website, www.consumerfed.org/fraud.

- **If you become a phishing victim, act quickly.** Contact your financial institution immediately if you think that the scammer may have gotten your payment card or banking information. If you believe you have become the victim of identity theft, you'll find information about what to do on Consumer Federation of America's www.IDTheftInfo.org website.