Consumer Education

Phishing Smishing and Vishing

CONSUMER EDUCATION

Communications Fraud Control Association

Version 1.0

Communications Fraud Control Association

Phishing Smishing and Vishing

Providing insights, knowledge and learning when it comes to fraud.

DEFINITION: A phishing scam is when a scammer uses technology (traditionally an email) to send a message to individuals with the goal of tricking that person into giving personal information or credentials for a specific platform that the scammer(s) is impersonating. The credentials sought can be in the form of passwords, account numbers, banking information, or social security numbers. In their communication, scammers will often use logos to make their messages appear more realistic. The organizations that the scammers attempt to impersonate are usually well-known entities that are well recognized brands, such as banks or online retailers.

TYPES OF PHISHING SCAMS

There are several variations of phishing scams that can be used, using a specific technology or platform. The more common variations include:

Smishing: Phishing scam that uses the format of SMS / Text messages. Using this platform, scammers send fraudulent text messages to any combination of 10 digit numbers (for the U.S.), making it the easiest way to send fraudulent messages and links to get the consumer to respond. Studies have shown that users read up to 98% of text messages, and respond to 45%, vs only 6% of email responses. (Source: www.trendmicro.com). This makes Smishing the more logical choice for scammers to use to defraud potential victims.

Vishing: Phishing scams where scammers impersonate reputable organizations such as financial institutions by making phone calls or leaving voicemail messages, to get the consumer to provide account numbers, PINs, and/or credit card numbers.
It is believed that most victims of Vishing scams tend to be older in age. **SOURCE**

MONEY FLOW/MOTIVATION

If scammers are successful in their attempt to defraud individuals, they will have gained access to account information such as account numbers, usernames, PINs, passwords, and potentially would be able to transfer funds out of the victim's accounts to send anywhere. The scammer will attempt to use these credentials to access other sites, such as popular large eCommerce organizations.

ADVICE / BEST PRACTICES*

Best practices for Individuals:

- Use and regularly update security software on your computer
- Use multi-factor authentication (2FA) on all of your accounts that offer it
- Avoid clicking on pop-ups
- Be suspicious of email attachments from known and unknown sources
- Do not engage in IMs from known and unknown sources that want you to click hyperlinks
- Only give out your personal information when YOU originate a phone call or web session to a site or number that is known to you ‘
- Regularly back up your data (external drive or cloud)

Do not reuse and recycle user id’s

Communications fraud is the use of telecommunications products or services with no intention of payment. Fraud negatively impacts everyone, including residential and commercial customers. The losses increase the communications carriers' operating costs. Although communications operators have increased measures to minimize fraud and reduce their losses, criminals continue to abuse communications networks and services. Therefore, communications operators tend to keep their actual loss figures and their plans for corrective measures confidential. Due to the sensitive nature of this topic, CFCA used a confidential opinion survey of global communications operators to support the global fraud loss study.

About CFCA

CFCA is a not-for-profit global educational association that is working to combat communications fraud. The mission of the CFCA is to be the premier international association for revenue assurance, loss prevention and fraud control through education and information. By promoting a close association among telecommunications fraud security personnel, CFCA serves as a forum and clearinghouse of information pertaining to the fraudulent use of communications services. For more information, visit CFCA at www.CFCA.org.

Correspondence should be sent to fraud@cfca.org

Disclaimer of Liability

www.cfca.org

Communications Fraud Control Association