Many Phish in the **Sea**

Office of Information Technology
Division of Information Security
AUGUST 2022

Fishing is an American pastime that has been around for hundreds of years and phishing is one of the oldest types of cyber-attack. While millions of Americans are out enjoying their summer fishing vacations, cybercriminals are enjoying a different type of phishing.

Fishing and Phishing may sound the same, but they are completely different. A major difference between fishing and phishing is that fishing occurs offline and phishing occurs online or via phone. You've been phished when cybercriminals attempt to steal your identity, money, or coerce you into providing personal information such as passwords or bank information on a seemingly legitimate website.

Not all fish are created equal; neither are all phishing attacks. This newsletter provides information on some common phishing attacks.

Email Phishing:
Email is the most common way cybercriminals phish because it is one of the easiest methods to use. Cybercriminals impersonate a legitimate company in an attempt to obtain login credentials and personal information by sending phishing emails. These emails normally use threats and a sense of urgency to frighten the users into doing what they want before those users have time to think it through.

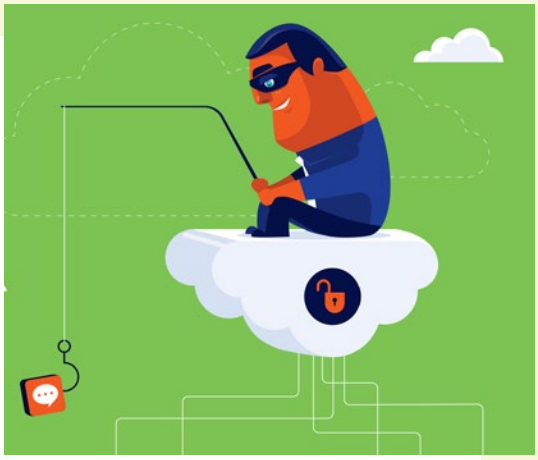
Whaling:
Whaling is a phishing attack that targets high-profile senior executives by sending sophisticated deceptive emails containing personalized information and tending to convey a sense of urgency. These emails often resemble correspondence from a trustworthy source, encouraging victims to click on a malicious embedded link.

Spear Phishing:
This type of phishing attack is more advanced because the cybercriminals usually personalize their attack emails with information specific to the victim to make the email appear more authentic. Spear phishing emails might contain information specific to the victim or their organization.

Angler Phishing:
Angler phishing is the newest type of phishing where the cybercriminal poses as customer support staff using social media platforms and accounts. The cybercriminal uses cloned websites, fake URLs, posts, tweets, and instant messaging to encourage people to download malware or divulge sensitive information. The cybercriminal's main goal is to trick dissatisfied customers into revealing personal details. This type of phishing is very effective because most customers that complain on social media expect the customer service representative to contact them online immediately. The customer is vulnerable due to being overwhelmed with frustration causing them to let down their guard to the cybercriminal.

Vishing:
Vishing is also known as voice phishing. Cybercriminals contact the target by making phone calls or leaving messages portraying themselves as a reputable company or government agency in an attempt to obtain personal information. Remember, legitimate government agencies will not contact you over the phone.

Smishing:
Smishing is known as Short Message Service (SMS) phishing. Cybercriminals send smishing texts including links that redirect victims to a phishing website to collect their personal information.



If a message or email…

- requests personal information
- states that there is a problem with your account or payment information
- states that they noticed login attempts or suspicious activity
- requests that you click on a link to make a payment
- requests you to download files or attachments

It could be a phishing attack!

If you receive any of the emails or messages described above, be cautious and confirm the message's legitimacy by contacting the directly rather than using a link or phone number provided in the message.

Phishing attacks are effective because the victims lack knowledge about the cybercriminal's techniques. To prevent successful attacks, people should educate themselves on phishing attacks and treat every email as a potential phishing email. If you notice a fraudulent social media account, report it to social media support and the real company immediately.

If the phishing incident occurred outside of work, you should report it to the following organizations:

- Cybersecurity and Infrastructure Security Agency (https://www.cisa.gov/uscert/report-phishing)
- Federal Trade Commission (https://reportfraud.ftc.gov/#/)
- FBI Internet Crime Complaint Center (https://www.ic3.gov/).

If you suspect a phishing incident has occurred at work, report it to the IHS Cybersecurity Incident Response Team at Incident@ihs.gov.

If you have any questions about this article, please contact Cybersecurity@ihs.gov.