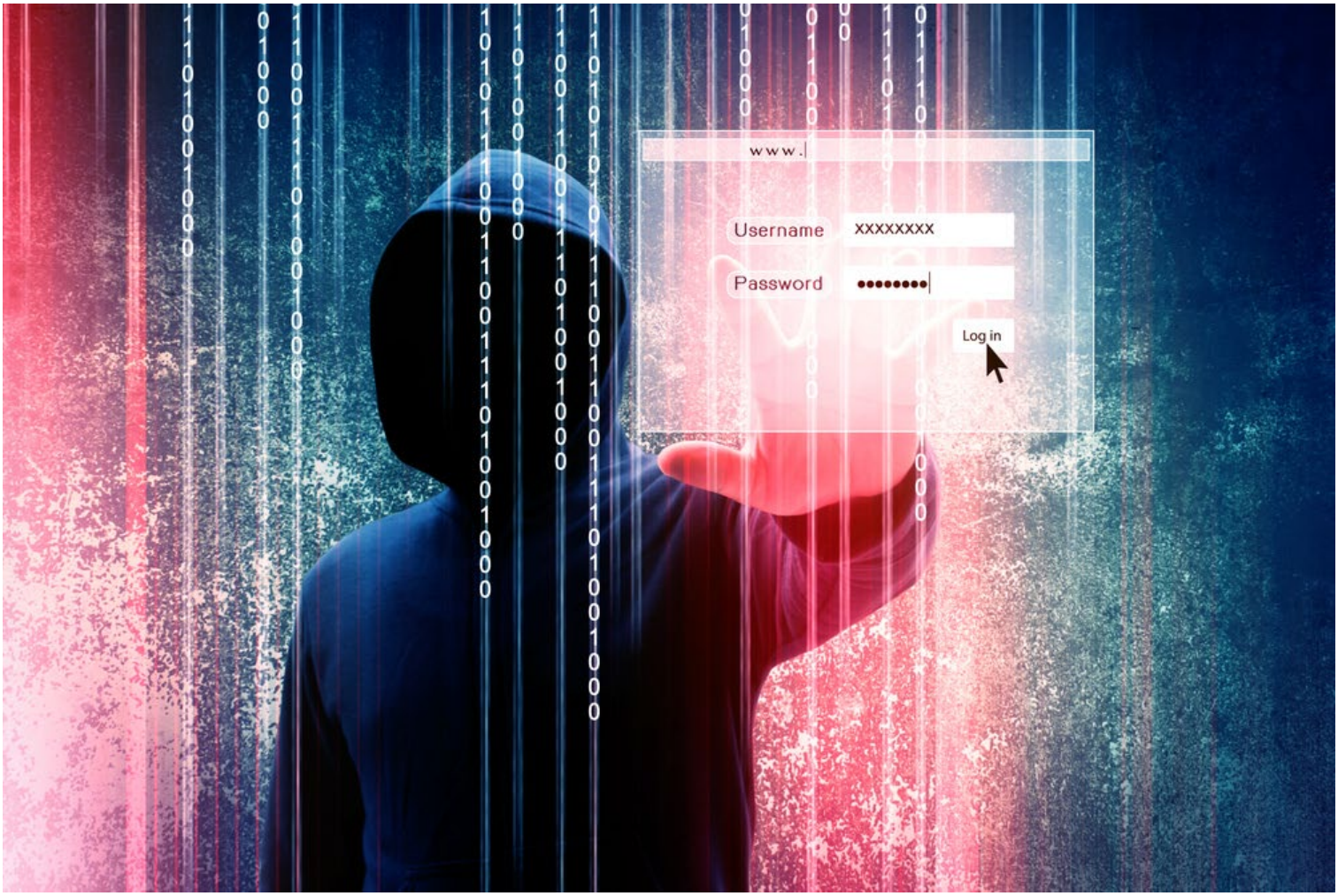
PHISHING INFORMATION

Introduction

You may have heard of the phrase, “there are plenty of fish in the sea,” and they’re absolutely right about that. Your digital life is an ocean full of information and hackers have learned that phishing is often times an easy way to earn their dinner.

Social engineering is a cybersecurity attack that relies on manipulating human behavior to steal information. Phishing is a subset of this type of attack that involves leveraging email, phone calls, or SMS/text. In the past, phishing attacks were easy to identify… a royal family member has passed and guess what, you’re getting the inheritance! Times have changed and so have the tactics these hackers use. From cloning legitimate emails to conducting investigations into your life, these hackers have become incredibly sophisticated.

Hackers will always cast their net, but you have the ability to prevent getting phished. Learn about the common types of phishing that are used, the psychology that they try to exploit, and how to ultimately recognize and avoid the net.



Common Phishing Types

There are many types of phishing attacks, but one singular goal – access to your sensitive data. From impersonation to cloning real emails, hackers will try everything in their arsenal to compromise your digital life. Understanding the different types of phishing attacks will help you defend yourself and others from them. Knowledge is the first step, so equip yourself with some of the common phishing types that hackers will employ.

Vishing

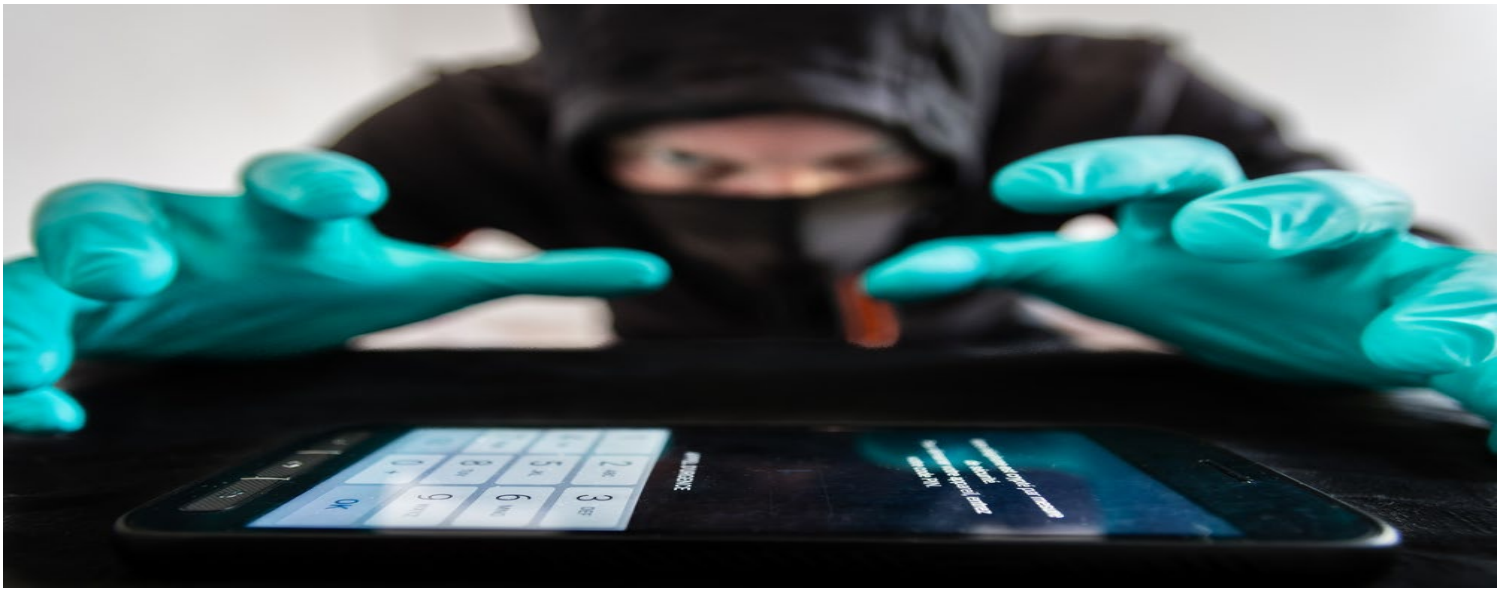
Vishing, short for "voice phishing" is when someone uses a voice call to try to steal information. Unlike the other phishing methods, vishing allows hackers to use their tone and emotion more clearly. Common tactics involve the attacker calling with claims to be a(n):

- Financial institution confirming unusual activity.
- Authority figure with of an arrest or warrant.
- Tech support attempting to fix a security issue.

Smishing

Smishing, short for "SMS phishing" is when someone uses the means of text message or SMS to try to steal information. People tend to let their guards down more when it comes to text messages. Common tactics involve the attacker messaging:

- A fake link to package delivery updates.
- A fake link for an overdue bill.
- Masquerading as a person the target knows.

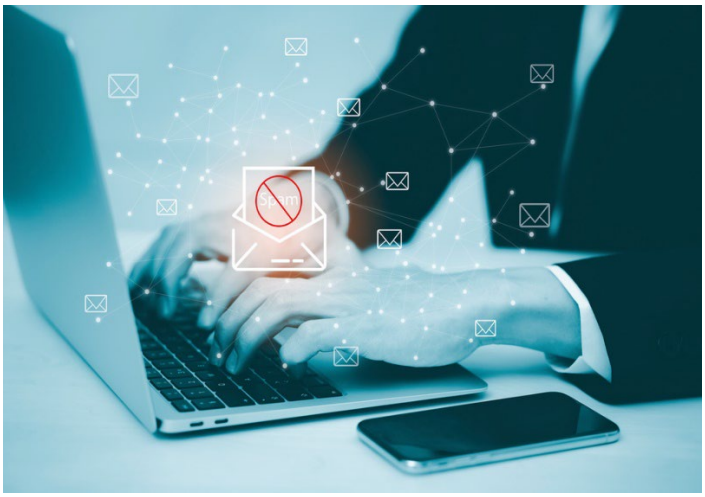


Whaling

This attack targets executive-level employees, “whales,” in an organization. These individuals often have access to sensitive data and/or finances, so a successful attack can result in large financial damage. Like spear phishing, reconnaissance is conducted to identify key targets.

Spear Phishing

This attack is directed at a specific individual, group, or organization. This form of attack involves a reconnaissance stage, where the attacker will first gather information about the target. Using this information, attackers are able to tailor their attack to the target, greatly improving chances of success.



Impersonation Phishing

This attack, now commonly referred to as “Business Email Compromise attacks,” involves attackers impersonating a trusted source, typically an executive-level employee. Common tactics involve the attacker impersonating:

- The CEO requesting the target purchase gift cards or transfer funds.
- A vendor the target works with and sending invoices to be paid.
- A service provider resetting credentials

Clone Phishing

This phishing method involves the attacker creating a near exact duplicate of a legitimate message to trick the target. The only difference may be that the links and attachments have been changed to a malicious version. The message may also be sent from an address that is very similar to the original, along with an explanation to the target why they may be receiving the “same” message twice. Common clones are created from automated emails from large service providers like Microsoft and Google.

Exploiting Psychology

Social engineering attacks aim to exploit what makes us humans. The kindness, trust, fear, and biases prevalent in our psychology make us who we are, but attackers can use this as a foothold for exploitation. Verizon's 2024 Data Breach Investigations Report found that 68% of breaches involved a human element. It is key to understand the aspects of human behavior that can be manipulated.

Authority

Attackers understand that people tend to follow and listen to authority figures. Doctors, teachers, government officials, bosses, even a trusted friend have sway over others. This belief can easily be taken advantage of. An attacker impersonating an authority hopes to exploit your trust.

Reciprocity

People typically believe in fairness; if someone does a favor for you, you're more likely to return the favor. An attacker may present you with a small gift such as a gift card to win favor. Once you accept the gift, you may be more inclined to click their (malicious) survey link.

Urgency

Fear and the sense of urgency are powerful drivers for action. Often times, this is used in combination with an authority figure. Under the pressure of impending threats, punishment, or financial loss, the target may hastily click a link or reply with sensitive information.

Consensus

An individual may have their own thoughts and beliefs, but within a group, those thoughts and beliefs may shift towards that of the majority. Studies have shown that we generally strive for consensus, sometimes overriding our individual opinions. Attackers may take advantage of this by stating that others have already complied with their request and evoke the belief of consensus.

Connection

People tend to be more open to people that they like or have rapport with. Factors such as attractiveness, commonality, compliments, and cooperation reinforce how much we like someone. The more you like someone, the more likely you are to let your guard down. Attackers can exploit this psychology by first building rapport with you or by masquerading as someone you may already like.

Scarcity

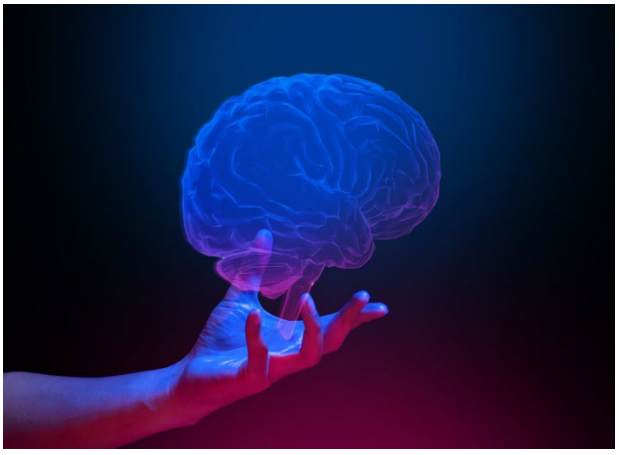
A common marketing tactic used against customers is scarcity. People are more likely to believe a product is good if its available for a limited time or there is limited supply. Attackers may lean into this by stating that there is limited stock left for an item, so click on this (malicious) link before time runs out.

Consistency

Most people value integrity, so we try to stay consistent with our prior engagements. Studies have shown that once a subject states their commitment to something, they are more likely to follow through. Attackers will try to take advantage of this by encouraging a small commitment and follow up with a more significant request in hopes they will follow through.

Recognizing Phishing

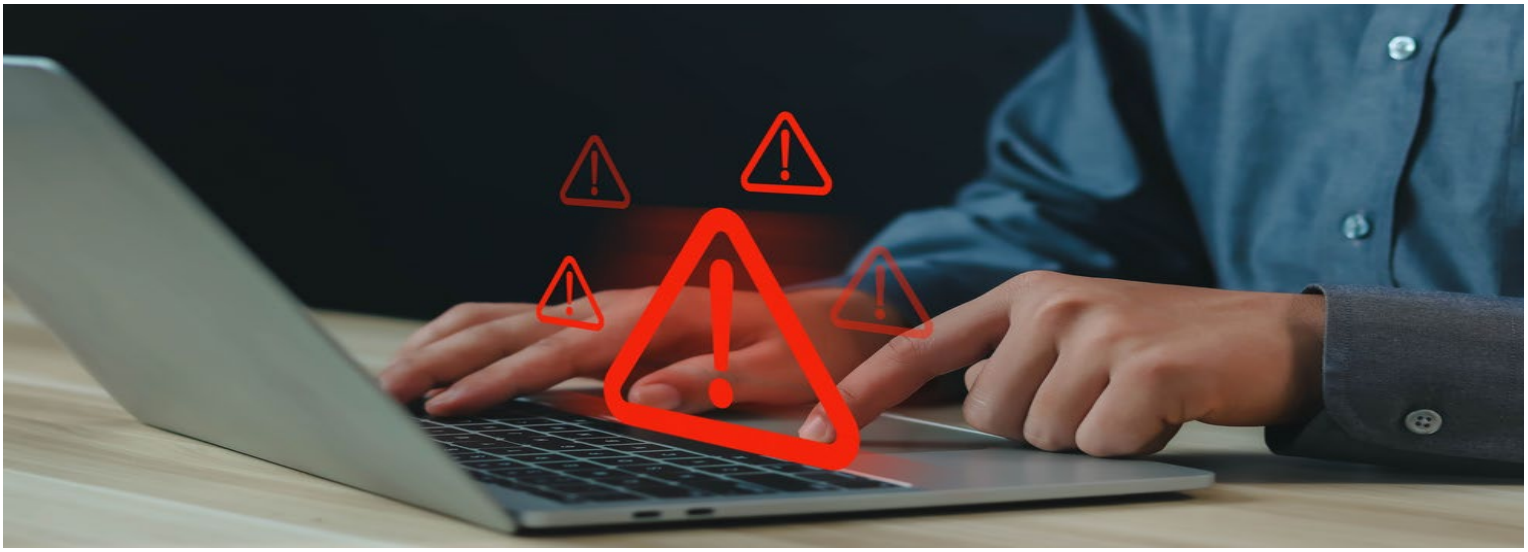
Your online accounts are gateways to your personal information. Whether it's your email, social media, or bank account, a successful phishing attempt can start a domino effect that could compromise your entire digital life. To better protect yourself, you'll need to arm yourself with the knowledge and a healthy dose of suspicion. Take a look at the how you can better recognize phishing.



Appeal to Psychology

When you receive a phone call or message, be sure to observe for appeals to your psychology. Attackers will often time combines different types of appeals and phishing tactics to manipulate their target. Here are some examples:

- If they are appealing to your sense of authority and urgency, they may be claiming to be police with a warrant.
- If they are appealing to your sense of connection and scarcity by being friendly and then offering a deal among friends.



Sender/Caller Information

One of the quickest ways to identify a phishing attempt is to look at the sender/caller information. However, it is important to know that these details can be spoofed, so if they pass this check, do not automatically assume it is safe.

- If it is a caller/texter, check to see if the number is correct.
- Check if the sender's name is correct.
- Check if the sender email is correct. Attackers may try to use similar email addresses and domains as the one they are impersonating.
- Check the email header and look to see if the sender IP is suspicious. If you're in California, the sender IP is from Russia, and they are claiming to be Microsoft, something may not be right.

Message Content

Typically, the biggest giveaway is found in the content of the messaging. Be sure to observe the following:

- Vagueness in greeting or message body. This may be indication of a generic phishing email that is sent to multiple people.
- Multiple typos. Legitimate emails TYPICALLY have limited to no typos.
- Alerts claiming suspicious activity or log-in attempts. Look for identifiers that indicate prove illegitimacy such as sender information, errors, and strange links.
- Incorrect contact info and/or signature. Cross-reference that information with information on an official website.

Context

Behind a valid action is a valid reason. Take into consideration the context of the situation and ask yourself, does this message or call make sense?

- New sender/caller. Does it make sense to receive communications from this new sender/caller? Does it make sense to receive an email that appears to be a chain from a new sender?
- Time. Does it make sense for this person to be calling or sending a message at the current time?
- Unsolicited. If the call or message is unsolicited, does it make sense for this person to be reaching out?
- Links, attachments, invoices, etc. Are you expecting to receive something from this person?

Links, QR Codes, and Attachments

These are typically the main pathways for an attacker to begin compromising your data. It's important to always be suspicious of these types of items, so consider the following before acting:

- Preview links. Before clicking on a link, hover over it to see where they take you.
- Shortened links. Some attackers will use link shortening sites to shorten their malicious links. There is no strong reason to use these because of hyperlinks. Avoid clicking these.
- QR codes. If you receive a QR code, you should be immediately suspicious. Though QR codes are now more popular, they can hide malicious websites. The camera on your device should allow you to preview the link and let you evaluate it before clicking on it.
- Attachments. Attackers will often attach malware to attachments such as PDFs. Be sure that you are expecting an attachment. Then scan the PDF with your antivirus. You can also use reputable security websites such as VirusTotal but understand the risk that if it is legitimate with your sensitive data, it will be uploaded to another party.

AI Tactics

AI has always been just a buzz word, but now it has evolved far beyond that. AI lets hackers generate perfect emails, mimic other people's voice, and even swap faces with others. At the time of this writing, AI is good, but not foolproof. Conduct these tests to help detect AI-based attacks.

Voice replication

- AI can't quite replicate emotion, so you can have the other person say a phrase with a specific emotion.
- Take note of how long responses are for each response and if the person can stop mid-sentence if you interrupt them. Have the person respond immediately to your questions.

Video face swapping

- Faces swapping can look realistic until clipping occurs. Have the other person move their head around in wide ranges of motion and look for distortions or clipping.
- Lighting is hard to replicate, so have the other person shine a light and note if there is a correct change on the face.