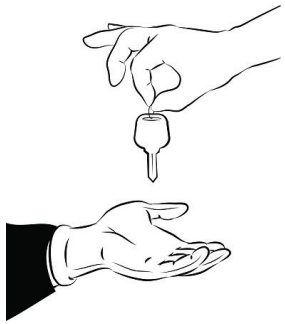
BELLEVUE UNIVERSITY

Phishing

What Is Phishing?

There are four main types of phishing:

1. Deceptive Phishing:



This is the most common type of phishing scam as hackers have found the easiest way to get access to accounts is simply by asking. Hackers send emails to end users that appear to be from a trustworthy source such as a legitimate company, the government, a bank, or **even your own IT department**.

The email is designed to manipulate the end user into providing sensitive information such as account logins, bank details, and other **personal information**. The email could ask you to click a link to input your information or open an attachment that infects your computer.

Hackers entice users to click on the link or open the attachment by making the email appear urgent, scaring the end user, or promising them some sort of reward. According to Verizon's "2016 Data Beach Investigations Report": "*The median time for the first user of a phishing campaign to open the malicious email is 1 minute, 40 seconds. The median time to the first click on the attachment was 3 minutes, 45 seconds*."

What Is Phishing?

2. Spear Phishing:

This type of phishing is similar to deceptive phishing, except rather than sending out emails to many end users, hackers target specific end users within your company. With spear phishing, hackers craft **highly targeted emails** by researching the end user through social media, blog posts, and other research methods. The email may even include information such as the user's name, position, company, work phone number, and other personal information.

For example, if a hacker finds an end user works with a specific company either within their **personal or professional lives**, they will target the user pretending to be that company, increasing the likelihood that the user will fall for the email. Phishing emails are **harder to detect** due to their customized approached and are therefore one of the most effective. In a recent survey of 300 companies, **84%** have had a spear phishing email penetrate their organization's security.

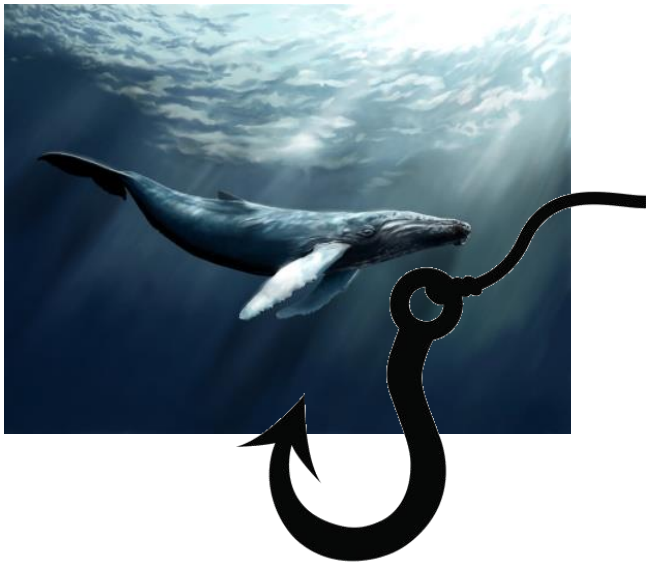
What Is Phishing?

3. Whaling:

Whaling is very similar to spear phishing but instead hackers target **senior executives** (the "big fish"). These emails are highly customized and usually take the form of **customer complaints**, legal subpoena, or executive issues. The 2008 FBI subpoena scam attacked around 20,000 corporate CEOs and approximately 10% fell for it.

4. Clone Phishing:

Similar to deceptive phishing, hackers attempting to gain sensitive information send emails that appear to be legitimate. The difference with clone phishing is rather than creating an email to pretend to be the legitimate source, they simply **copy (clone) an existing email** that has already been sent and replace the attachment or link with a malicious one. The email will claim to have been **resent or updated** to disguise it from the recipient.



How Does It Affect You and Your Organization?

The consequences of a phishing campaign **depend on the hacker's intent**. If when the link or attachment is opened, malware is downloaded onto your computer, the malware cannot only take **control of your computer** and have access to all your personal data on it, but also **spread through your network** to the entire organization. The hacker now has the ability to find all the sensitive data they require within the organization. This can include **customer credit card numbers**, other logins, and much more.

If the phishing email asked for your organization account login, the hacker now has the ability to log into your organization's systems and browse while pretending to be you. This allows the hacker to pass through **undetected**. This is one of the **most powerful tools** for a hacker and one of the main reasons humans are targeted.

Finally, if the hacker is able to obtain personal information such as your social insurance number, bank account details, etc. they now have **access to your personal life**. The hacker has the ability to control your personal assets, which they can block you from using, steal from, and much more.

Threat Identification

Best practices to identify phishing emails:

- ❑ Be suspicious of emails that ask for your personal information.
- ❑ Check the sender's email address. Is it exactly the same as the company's email address or similar? If you are unsure, **search for the email address** to see if it is legitimate.
- ❑ Always look at the greeting. Common phishing uses phrases such as "Valued Customer." **However, the hacker may use your name if you have been spear phished!**
- ❑ [Organization name], legitimate banks, and most other companies will **never** ask for your personal credentials via email.
- ❑ Look for bad spelling and grammar in the text of the email.
- ❑ Review the signature. Does it look legitimate or provide contact information?
- ❑ Does it make sense for the email to have an **attachment**. Be wary of .exe attachment files.
- ❑ **Watch out** for common phishing practices listed on the next slide.

A Hacker's Common Practices

Common phishing emails:

- Have a sense of **urgency**. Hackers word emails to include a sense of urgency to make you react quickly, reducing your time to think and realize the scam.
- Ask you to change your account information because there is a **discrepancy** with your account or you need to **verify** your account. This tactic is used to scare the end user into clicking on a bad link or going to a bad site and filling in their account information.
- Tell you your account has **been hacked**. This is used to get a similar response as the one above. You are less likely to think an email that announces you have been hacked is a phishing email.
- Ask for a wire transfer or the details of a failed wire transfer for a compelling reason. The email usually claims the "transfer details" are in the attachment, which is malware.
- Want to send you **money**, ask you to donate money, or say you have won a prize. They will either ask for your personal information to send you money, open the attachment to receive the invoice, or click a link to claim your prize.
- Include logos, brand names, and slogans of legitimate companies. This is used to create a sense of trust with the end user.

Be Proactive

How to avoid being phished:

- ✓ **Do not** click links, open attachments, or fill out forms in suspicious emails. Instead, you can type in the URL to the company's website or search for it.
- ✓ **Hover over the link** before clicking on it to make sure it's taking you where it says it will take you. Check the website: Is it http or https? Is it spelled correctly? Is it the company's website? Some links may be legitimate so make sure you **check them all**.
- ✓ If you click the link and are unsure if it is real or fake, put a **fake password first**. If it appears you have signed in, then you are probably on a phishing site.
- ✓ Keep your web browser up to date and use anti-phishing detection plug-ins or add-ons.
- ✓ **Never** provide personal information through an email.
- ✓ **Reach out** to the person/company that emailed you directly. They will tell you if the email is valid or not.
- ✓ Don't open email attachments that you didn't expect to receive.

Reporting and Contact Information

If you have any general questions:

– Bruin Support Services at 1.800.756.7920

Resources

Print the checklist below to remind you what to look for.

Phishing checklist:

- ❑ Does the email ask for your personal information?
- ❑ Check the sender's email address.
- ❑ Is the greeting personal?
- ❑ Is there poor spelling and grammar in the email?
- ❑ Does the signature look legitimate and have contact information?
- ❑ Is the attachment necessary?
- ❑ Does the attachment end in .exe?
- ❑ Hover over all links to make sure they will lead you to the right place.
- ❑ Are there any clear signs of common phishing tactics?
- ❑ Are there any other signs that this is a fake email? Do you feel it is suspicious? If so, report it or contact the company directly.

A private, non-profit institution founded in 1966, Bellevue University is accredited by the Higher Learning Commission through the U.S. Department of Education. For general information, please call 1.800.756.7920.