Cybersecurity Awareness Month: All About Phishing!

Walker Sigler, Ali Cochran, and Justin Nelson

What is Phishing?

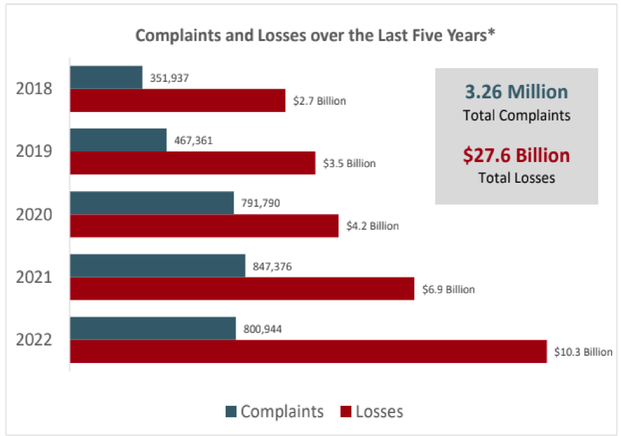
Phishing takes place when a user is contacted by an illegitimate party posing as a legitimate institution in an attempt to obtain sensitive information.

Early phishing techniques can be traced back to the 1990s, as demonstrated on the platform AOL.

Phishers began riding a large wave of success between the years of 2004-2005, as about 1.2 million users fell victim to phishing, totaling $929 million in damage.

Today, according to phishing.org, organizations lose about $2 billion per year to phishing scams.

https://www.phishing.org/



https://www.techopedia.com/phishing-statistics

How to Recognize Phishing Scams

Phishing scams may be easy or difficult to identify, depending on who the attacker is. The following criteria may indicate the possibility of a phishing scam:

- Email addresses that mimic legitimate organizations: Oftentimes, these addresses contain misspellings.
- Generic greetings such as "Dear User" or "Dear Customer" instead of addressing users by their name.
- Requests for personal or financial information, as legitimate organizations will not ask for sensitive information such as passwords or credit card information.
- Look for poor grammar, spelling errors, and inconsistent formatting.
- The content in the attack may be vague.

https://www.cisa.gov/sites/default/files/2023-02/phishing-infographic-508c.pdf

How to Protect Against Phishing Attacks

Multiple preventative measures can be taken to ensure that you are protected from various types of attacks. Here are some suggested by FTC.gov:

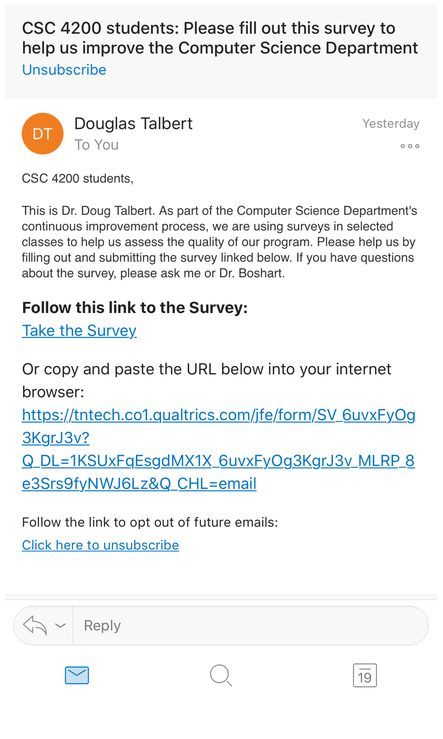
- Install security software. Security software can monitor the inflows and outflows of data on your computer, determining what is safe and what is potentially risky.
- Adjust your device settings so that system updates and software updates are performed automatically. Keeping everything up-to-date helps ensure that new types of attacks will not affect the integrity of your device's data.
- Get comfortable with and enable multi-factor authentication. Multi-factor authentication is a safeguard for a login process which requires more than just a password to log into an account. For example, a 2-factor login process can include typing in a passphrase then scanning a fingerprint. This multi-step process makes it significantly harder for attackers to interfere with important information and property.

Phishing Attempts Through TTU

You've almost definitely come in contact with phishing scams before, but did you know they're prevalent, even in your own school? You may think that trusting and responding to messages that appear in your school email inbox is a good idea, but they can't always be trusted! Fake work studies, job opportunities, surveys, and more are actually very common! Even in your school email!

Here are a few ways to protect yourself against scams like these:

- Don't trust unsolicited emails, especially if they ask for personal information.
- Verify the sender. If unsure, contact and confirm authenticity.
- Be cautious of generic greetings or misspellings.
- Don't click on suspicious links or attachments.


CSC 4200 students: Please fill out this survey to help us improve the Computer Science Department
Unsubscribe

DT Douglas Talbert
To You
Yesterday

CSC 4200 students,

This is Dr. Doug Talbert. As part of the Computer Science Department's continuous improvement process, we are using surveys in selected classes to help us assess the quality of our program. Please help us by filling out and submitting the survey linked below. If you have questions about the survey, please ask me or Dr. Boshart.

Follow this link to the Survey:
Take the Survey

Or copy and paste the URL below into your internet browser:
https://tntech.co1.qualtrics.com/jfe/form/SV_6uvxFyOg3KgrJ3v?Q_DL=1KSUxFqEsgdMX1X_6uvxFyOg3KgrJ3v_MLRP_8e3Srs9fyNWJ6Lz&Q_CHL=email

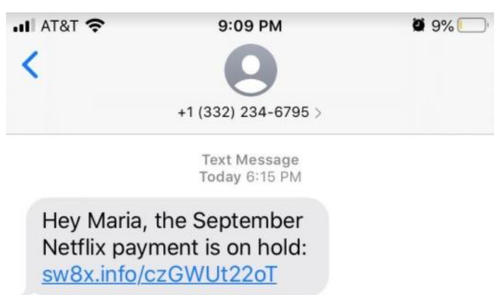
Follow the link to opt out of future emails:
Click here to unsubscribe

Reply

Phishing Fun Facts

- The name "phishing" is derived from the word fishing, as hackers are fishing for information.
- Phishing often relies solely on social engineering tactics.
- The "Nigerian Prince" Scam is one that has been around for decades!
- Google blocks around 100 million phishing emails daily.

https://aag-it.com/the-latest-phishing-statistics/

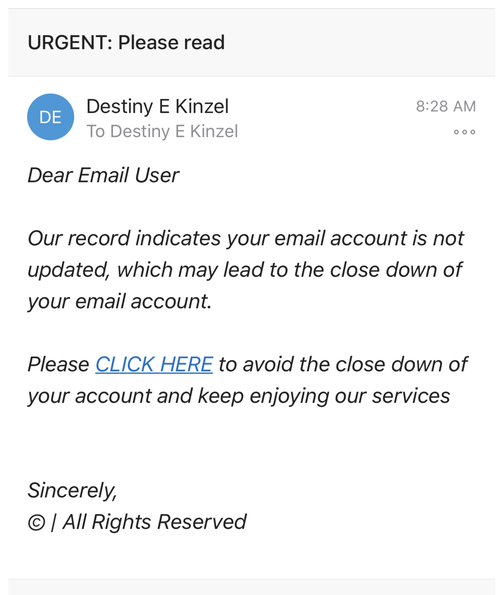


Types of Phishing Scams

There are numerous types of cyber phishing scams. Here are a few common types to know:

- Email Phishing – Extremely common. Attackers pose as trusted organizations and trick recipients into divulging personal information.
- Spear Phishing – A targeted phishing attack. Attackers research and craft highly personal messages to seem more reputable.
- Vishing (Voice Phishing) - Attackers use phone or voice calls to impersonate trusted sources.
- Smishing (SMS Phishing) - Attackers send fraudulent text messages to the victim's phone. They may contain malicious links or requests for personal information.
- Pharming - These attacks manipulate the victim's DNS settings or domain to redirect them to fake websites to steal login credentials or other sensitive data.
- Clone Phishing - These attacks attempt to clone an email the victim has already received but with malicious links or attachments.
- Man-in-the-Middle (MitM) Phishing - The attacker intercepts communication between the victim and a trusted entity to steal sensitive information
- Search Engine Phishing - Scammers create fake websites modeled after real ones, tricking users into entering sensitive information.

ChatGPT by OpenAI was used to help create this list.
Prompt: "list common types of phishing attacks"


URGENT: Please read

DE Destiny E Kinzel
To Destiny E Kinzel
8:28 AM

Dear Email User

Our record indicates your email account is not updated, which may lead to the close down of your email account.

Please CLICK HERE to avoid the close down of your account and keep enjoying our services

Sincerely,
© | All Rights Reserved