Phishing steals identities , data and wrecks live. It affects everyone . The worst part is that through phishing is now more than a decade old , many people are not familiar with how it works and sadly still fall vitims for this scam.

Prevent youself from being *phishing*

What is phishing?

- Phishing is one of the most popular attack vectors and will likely remain so for the foreseeable future. Why is phishing so challenging to mitigate? Because instead of attempting to bypass modern security tooling, phishing exploits the much more straightforward and well-known vulnerabilities of human beings. As phishing is using data for what? Using data to access a victim’s account or even to open fake bank accounts or credit cards in the victim’s name. Added to that phishing is using the victim’s computer system to install viruses and disseminating phishing emails.

Phishing's Types

- ***Phishing*** ***involves an attacker trying to trick someone into providing sensitive account or other login information online. All the different types of phishing are designed to take advantage of the fact that so many people do business over the internet. This makes phishing one of the most prevalent cybersecurity threats around, rivaling distribuated denial- of-service(DDoS) , data breaches , and many kinds of malware. Here is some different types of phishing attacks:***

  - Spear phishing involves targeting a specific individual in an organization to try to steal their login credentials **.**The attacker often first gathers information about the person before starting the attack, such as their name, position, and contact details.

  - Vishing , which is short for "voice phishing," is when someone uses the phone to try to steal information. The attacker may pretend to be a trusted friend or relative or to represent them.

  - In an email phishing scam, the attacker sends an email that looks legitimate, designed to trick the recipient into entering information in reply or on a site that the hacker can use to steal or sell their data.

  - An HTTPS phishing attack is carried out by sending the victim an email with a link to a fake website. The site may then be used to fool the victim into entering their private information.

How to spot an attacks?

- ***These are just a few ways that a scammer will try to trick you into clicking a link or opening a dangerous attachment. You always want to pay attention to a few key details when trying to determine if an email is safe or not. Look at factors like:***

  - Who is sending the email- If you don't immediately recognize the sender, you'll want to see if the person or business name is spelled correctly.

  - Subject Line- Always examine the subject line of an email before opening or responding to it.

  - Any suspicious links or attachments- Phishing emails often include outbound links that will redirect you to a page that is broken or not a true URL.

  - The type of content in the email – Examine the overall tone of the email.

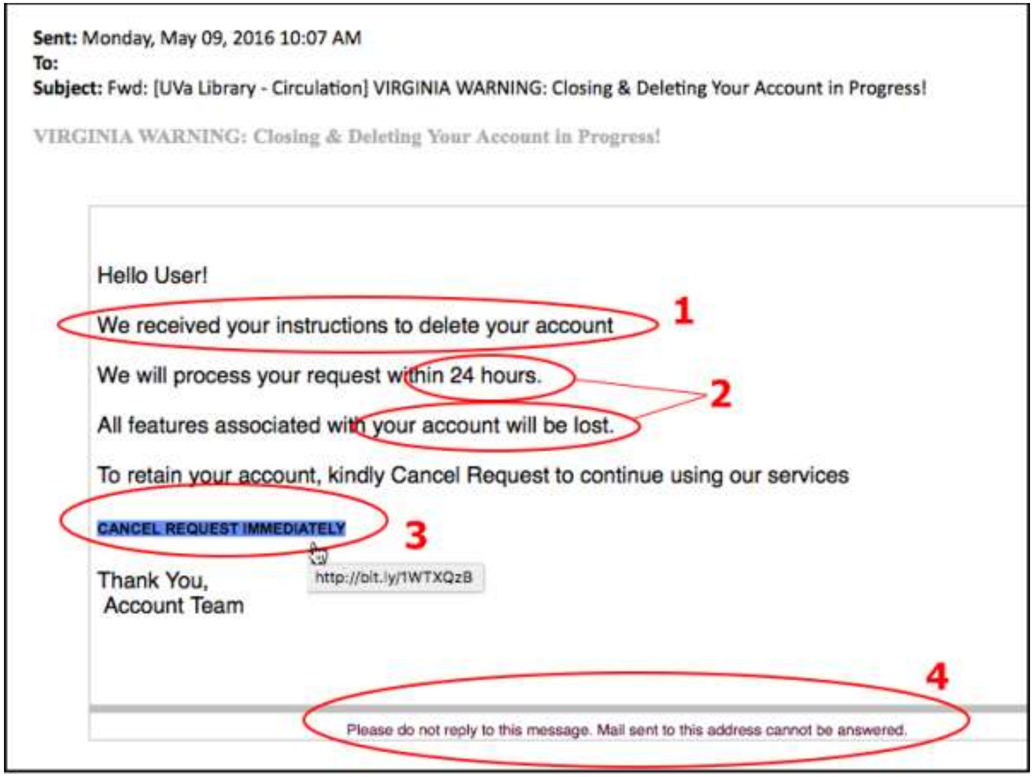
How To Protect Yourself From Phishing Attacks?

- ***While we would love to think that our email provider is perfect and will automatically filter out any suspicious or wanted emails, that's not always the case. Scammers have gotten better at outsmarting the spam filters which makes it easier for them to make their way to your inbox. It's always a good idea to have a few extra layers of protection to prevent phishing attacks:***

  - Think before you click on any links!
  - Keep informed about phishing techniques.
  - Install an Anti-Phishing toolbar.
  - Verify a Site's Security.
  - Check your online accounts regularly.

The most common examples of phishing emails:

- The fake invoice scam.
- Email account upgrade scam.
- Advance-fee scam.
- Google Docs scam.
- PayPal Scam.
- Message from HR scam.
- Dropbox scam.
- The council tax scam.



Sent: Monday, May 09, 2016 10:07 AM
To:
Subject: Fwd: [UVa Library - Circulation] VIRGINIA WARNING: Closing & Deleting Your Account in Progress!

VIRGINIA WARNING: Closing & Deleting Your Account in Progress!

Hello User!

We received your instructions to delete your account

We will process your request within 24 hours.

All features associated with your account will be lost.

To retain your account, kindly Cancel Request to continue using our services

CANCEL REQUEST IMMEDIATELY

http://bit.ly/1WTXQzB

Thank You,
Account Team

Please do not reply to this message. Mail sent to this address cannot be answered.