
SECURITY AWARENESS

- Knowledge and attitude of an individual, a group of people, an organization to protection of assets (physical, information, economic) of the individual, the group of people, the organization.

- The knowledge and attitude members of an organization possess regarding the protection of the physical, and especially informational, assets of that organization.

- The perception by individuals within an organization that **security** is important to the conduct of business

https://www.igi-global.com/dictionary/security-awareness-in-the-internet-of-everything/26091

Helps to minimize risk thus preventing the loss of Personal Identifiable Information (PII), Intellectual Property (IP), money or brand reputation.

- Personal Identifiable Information (PII) - any representation of information that permits the identity of an individual to whom the information applies to be reasonably inferred by either direct or indirect means.

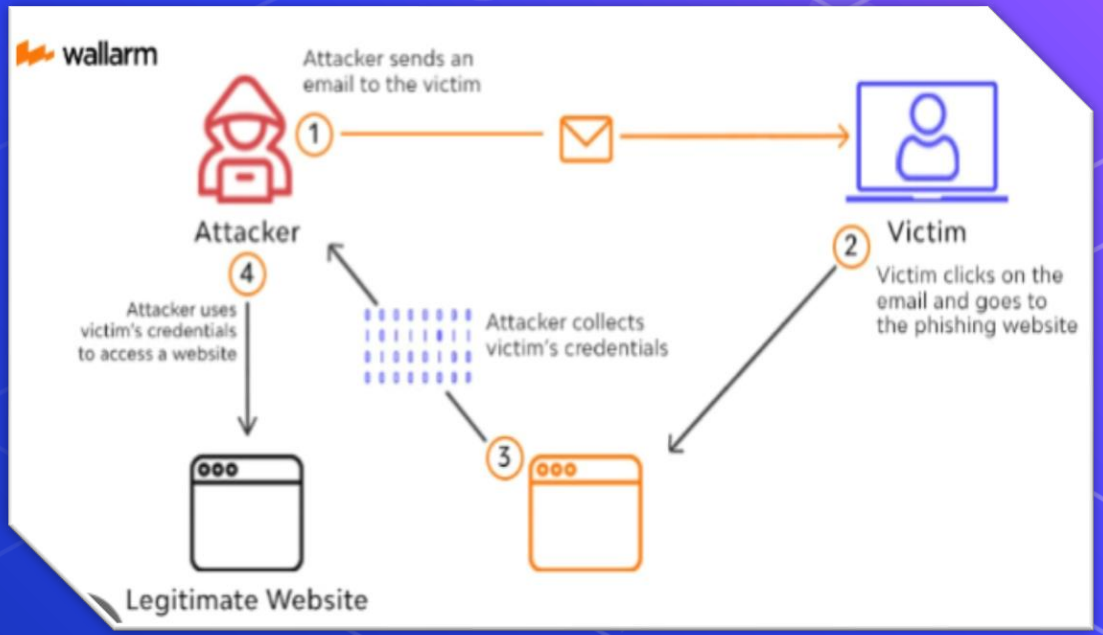
- Intellectual Property (IP) - refers to creations of the mind. It can be an invention (patent / utility model), a design (industrial design), a brand name (trademark, or a literary and artistic work (copyright).

*An effective awareness training program addresses the cybersecurity mistakes that people may make when using email, the web and in the physical world such as tailgating or improper document disposal.

12 Most Important Security Awareness Topic for 2023

1. Phishing Attacks

- when attackers attempt to trick users into doing 'the wrong thing', such as clicking a bad link that will download malware, or direct them to a dodgy website.




5 Common Types of
Phishing Attacks

- Bulk Phishing is when the attacker sends a large number of untargeted phishing emails, often impersonating banks or financial service providers, to individuals and employees.
- The most common type of phishing attack.

- Spear Phishing takes a more targeted approach. The email will include tailored communication to target a specific organisation, or even a specific individual in an organisation.
- This can make it appear more like a legitimate email.

- Like spear phishing, whaling is targeted approach, with the attacker's sights set on the 'big fish'.
- A whaling phishing attack targets specific executives, high-level decision makers, CEOs, and CFOs, for example, in an individual organisation.

- Vishing (also known as voice phishing) uses the telephone or VOIP system.
- The attacker will often call multiple telephone numbers, mimicking a bank or other trusted organisation, and play a recorded message about an issue with an account or credit card.
- They will then attempt to encourage the victim to call another number to ‘resolve the issue’, where they will then ask for sensitive information.

- Smishing (also known as SMS phishing) uses text (SMS) messages to target individuals.
- Similar to email phishing, the message will ask the victim to click a link, call a phone number, or contact an email address, where they will often be asked to share sensitive information.

What is a Phishing Email?

- A phishing email is a cyber attack that relies on deception to steal confidential information from users and organizations.
- Phishing victims are tricked into disclosing information that should be kept private. When a phishing email arrives, recipients have no reason to doubt the request. They believe that the party requesting the information – often posing as a familiar platform, a trusted vendor, colleague, or boss – is who they say they are. With the best intentions, phishing email victims respond without a second thought.

What is a Phishing Email?

- In phishing emails, cyber criminals often ask for the following information:
  - Date of birth
  - Social security number
  - Phone number
  - Home address
  - Credit card details
  - Login details
  - Password (or other information needed to reset your password)

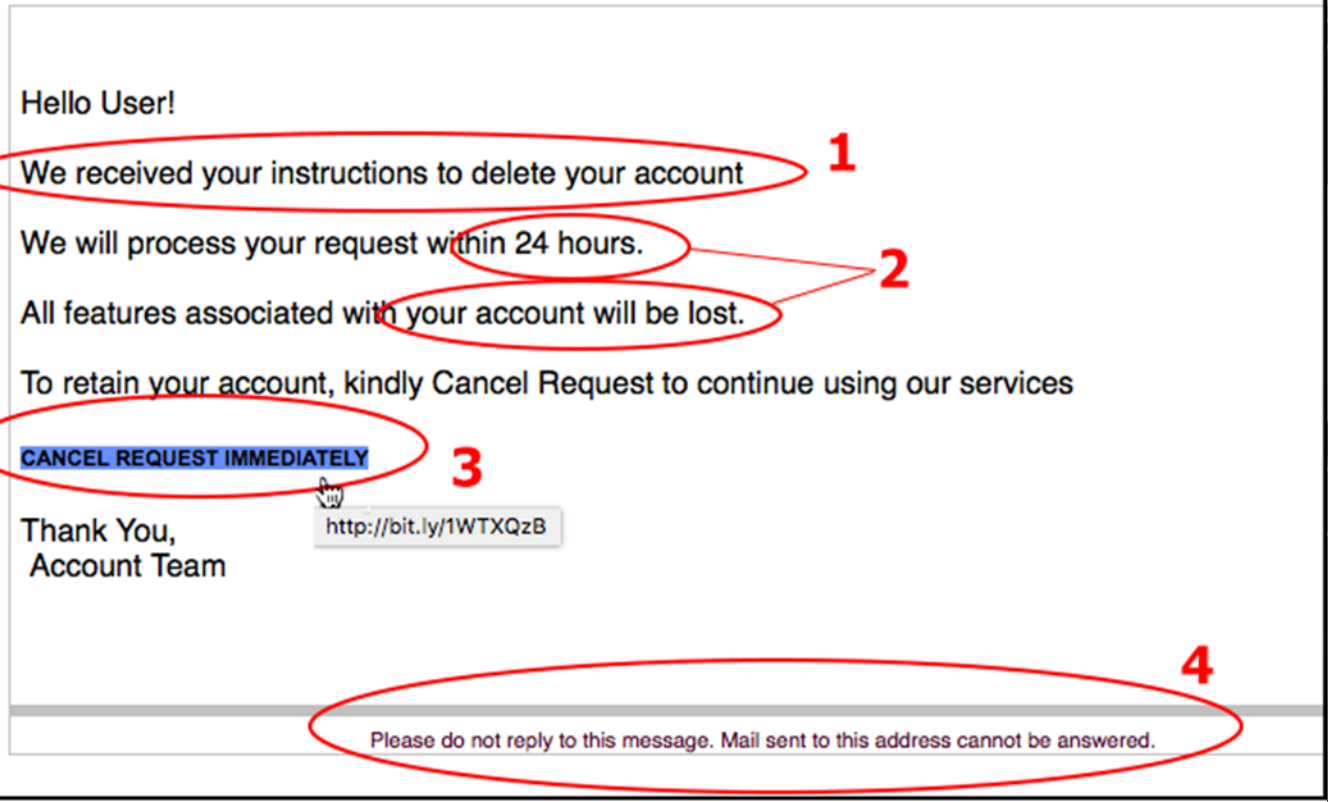
- Cyber criminals then use this information to impersonate you and apply for credit cards or loans, open bank accounts, and commit other fraudulent acts.
- Some cyber criminals use the information collected in an initial phishing email to launch more targeted cyber attacks, such as spear phishing or business email compromises (BEC), that rely on knowing more about the victim

How Does Phising Happen?

- Phishing happens when a victim acts on a fraudulent email that demands urgent action:
- Examples of requested actions in a phishing email include:
    - Clicking an attachment
    - Enabling macros in a word document
    - Updating password
    - Responding to a social media friend or contact request
    - Connecting to a new Wi-Fi hot spot

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!



From: u652193196@srv98.main-hosting.eu [mailto:u652193196@srv98.main-hosting.eu] **On Behalf Of** UVa Help Desk
Sent: Monday, September 12, 2016 1:15 PM
To: caruccio@virginia.edu
Subject: Renewal UVa Computing ID

Dear User,

University Information Security policy requires all internet passwords to expire 6 months from the date they are set. You are receiving this notice because your UVa computing ID password will expire soon. 1

For uninterrupted access, you must reactivate your account before the current one expires. For this purpose, you just need to follow the instructions in the link below. After your successful authentication, you will be redirected to the university services homepage.

https://netbadge.virginia.edu/myaccount/reactivation.html

!

http://university-system.cf/services/activation/link.php?M=389&N=20&L=7&F=H

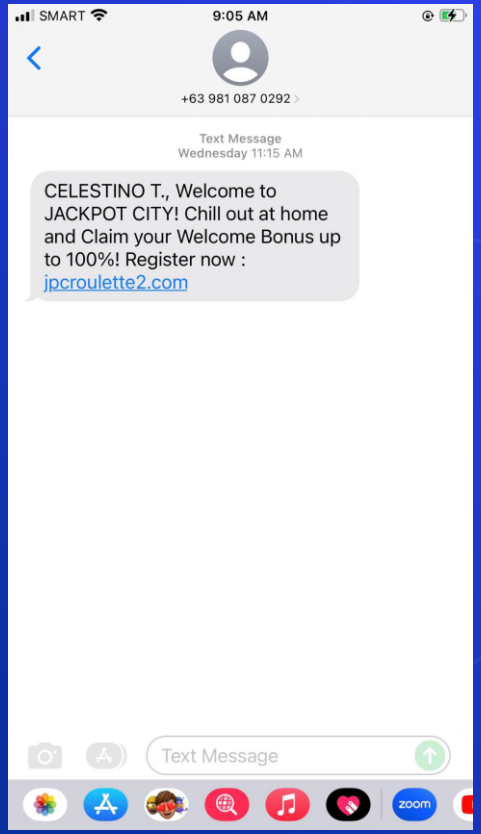
Please note: if you do not reactivate your account applications that require it for access. When you attempt to log in to these applications, you will receive a prompt to contact the UVa Help Desk. After the activation is done, your access will be immediately restored.

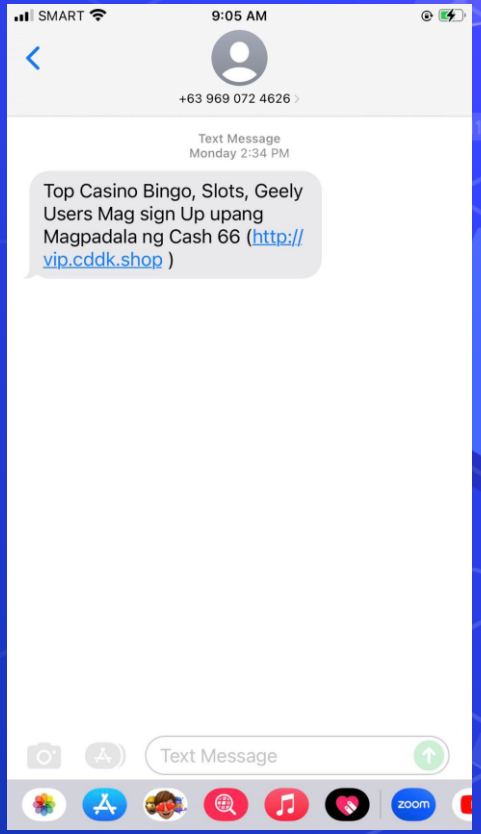
If you have any questions, need assistance, or cannot remember your current login password, please contact the UVa Help Desk at 4help@virginia.edu or contact your college or department's technical support. 2

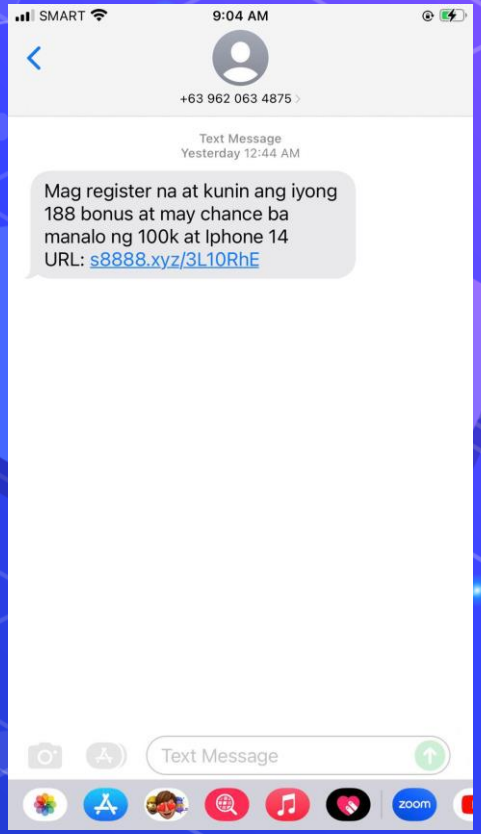
Best Regards

UVa Help Desk | © The University of Virginia

Examples of Smishing







5 Steps to Protect against Phising Email Attacks

- **1. Educate:** Use security awareness training and phishing microlearnings to educate, train, and change behavior.
- **2. Monitor:** Use phishing simulation tools to monitor employee knowledge and identify who in the organization is at high risk for receiving or responding to a phishing attack.
- **3. Communicate:** Provide ongoing communications and run campaigns about phishing emails, social engineering, and cyber security.
- **4. Incorporate:** Make cyber security awareness campaigns, training, support, education, and project management part of your corporate culture.
- **5. Apply:** As end users, apply this knowledge about phishing email attacks in your everyday activities. Be aware of the risks and take the time to assess emails, texts, and websites.