

PHISHING AWARENESS TRAINING

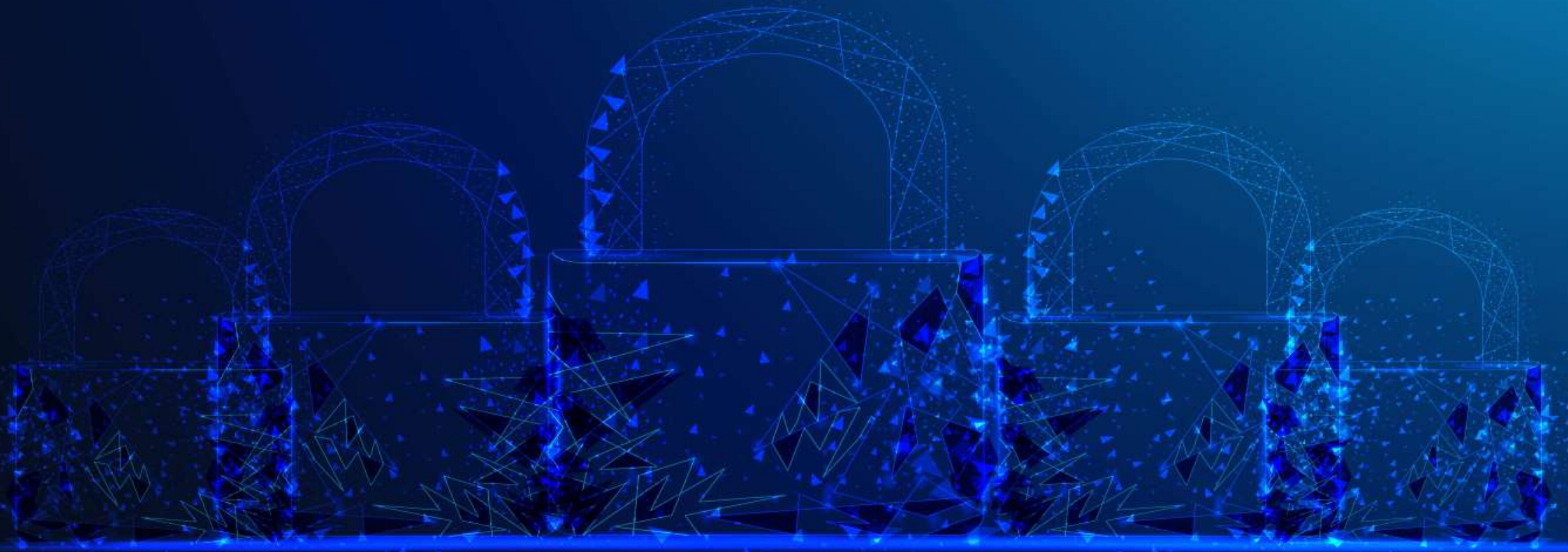


Table of Contents

- Cybersecurity Introduction
- What is Phishing?
- Types of phishing attacks
- Recognizing & Avoiding phishing attacks(emails, websites, and social engineering tactics)
- Secure Your Devices from Phishing attacks
- How do we stop getting phished?



What is Cybersecurity?

- The technique of protecting internet-connected systems such as computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks is known as cybersecurity.
- We can divide cybersecurity into two parts one is cyber, and the other is security.
 - “Cyber” refers to the technology that includes systems, networks, programs, and data.
 - “Security” is concerned with the protection of systems, networks, applications, and information. In some cases, it is also called electronic information security or information technology security.
- A cybersecurity threat, or cyberthreat, is an indication that a hacker or malicious actor is attempting to gain unauthorized access to a network for launching a cyberattack.

Types of Cyber Security Threats

- Malware attack
 - Trojan virus, Ransomware, Wiper malware, Worms, Spyware, Fileless malware, Application or Website manipulation.
- Social engineering attacks
 - Phishing, Spear phishing, Malvertising, Drive-by downloads, Baiting, Vishing, Whaling, Pretexting, Pharming, etc.
- Software supply chain attacks
 - Compromise of software build tools or dev/test infrastructure, Compromise of devices or accounts owned by privileged third-party vendors, Malicious apps signed with stolen code signing certificates or developer IDs, Malicious code deployed on hardware or firmware components, Malware pre-installed on devices such as cameras, USBs, and mobile phones
- Advanced persistent threats (APT)
- Distributed denial of service (DDoS)
- Man-in-the-middle attack (MitM)
- Password attacks

What Is Phishing?

- Phishing is a type of social engineering attack where a cybercriminal uses email or other text-based messaging to steal sensitive information. By using a believable email address, an attacker aims to trick the target into trusting them enough to divulge personal data, such as login credentials, credit card numbers, or financial account info.


Example

- An individual receives an email from his or her bank (for example, Chase).
- The email appears to be sent from Chase, with the Chase logo embedded in the email.
- The email explains how there is an urgent issue with the individual's account, instructing her to click on a link to address the matter right now.
- Once the individual clicks on the link, she is brought to a webpage which mimics that of Chase.
- Unknowingly, the individual enters her username and password to enter the website.

Types of Phishing Attacks

- Spear Phishing
 - General email attacks use spam-like tactics to blast thousands at a time, spear phishing attacks target specific individuals within an organization.
- Whaling
 - Phishing attack targeted towards high profile executives, that is disguised as a permitted email.
- BEC (Business Email Compromise)
 - Phishing attack that primarily targets senior executives and finance department staff.
- Clone Phishing
 - Where the scammer creates an almost-identical replica of an authentic email, such as an alert one might receive from one's bank, in order to trick a victim into sharing valuable information.
- Vishing
 - voice phishing (vishing) attacks use social engineering techniques to get targets to divulge financial or personal information over the phone.

Recognizing & Avoiding phishing emails

- There are a few tell-tale signs that help you identify phishing emails. Knowing what they are is essential to recognize phishing:
 - Public domain email address says phishing alert
 - Misspelled email addresses
 - Sender's name doesn't match email address
 - Sense of urgency and pressure
 - Trustworthy brands mind the spelling
 - Shortened links
 - Counterfeit branding and logos
 - Forged signature red flags
- 
- The background of the slide is a deep blue gradient. It features several large, semi-transparent wireframe cubes arranged in a row, receding into the distance. These cubes are composed of thin blue lines forming their edges. Scattered throughout the scene are numerous small, solid blue triangles of various sizes, some pointing towards the viewer and others away, creating a sense of depth and movement. The overall aesthetic is futuristic and digital, fitting the theme of cybersecurity and phishing.

Recognizing & Avoiding phishing emails

- Suspicious looking source email address

From: mastercardsIT@gmail.com

To: employee@email.com

Subject: URGENT! Password Reset Required

—

Body:

Hello (insert name),

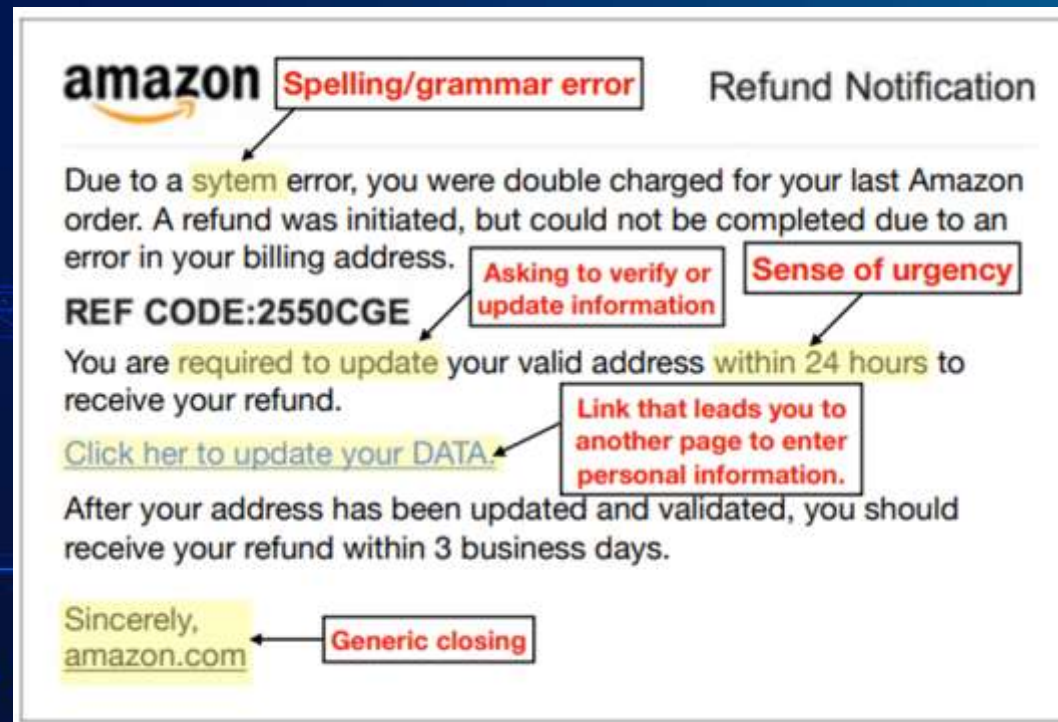
Your email account has been compromised. immediate action is required to reset your password!

Click here to reset your password in the next hour or your account will be locked:

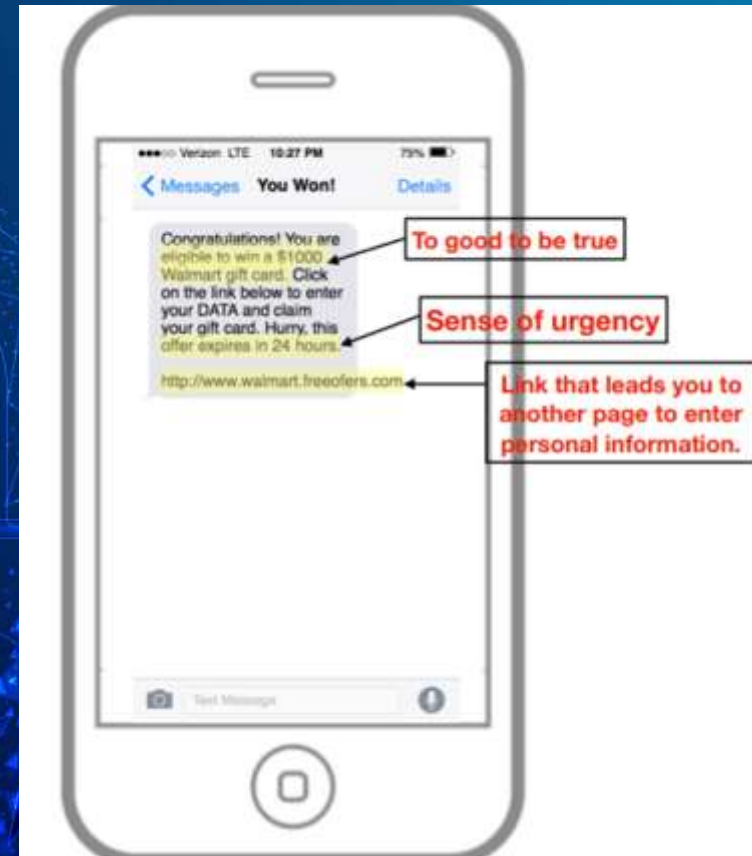
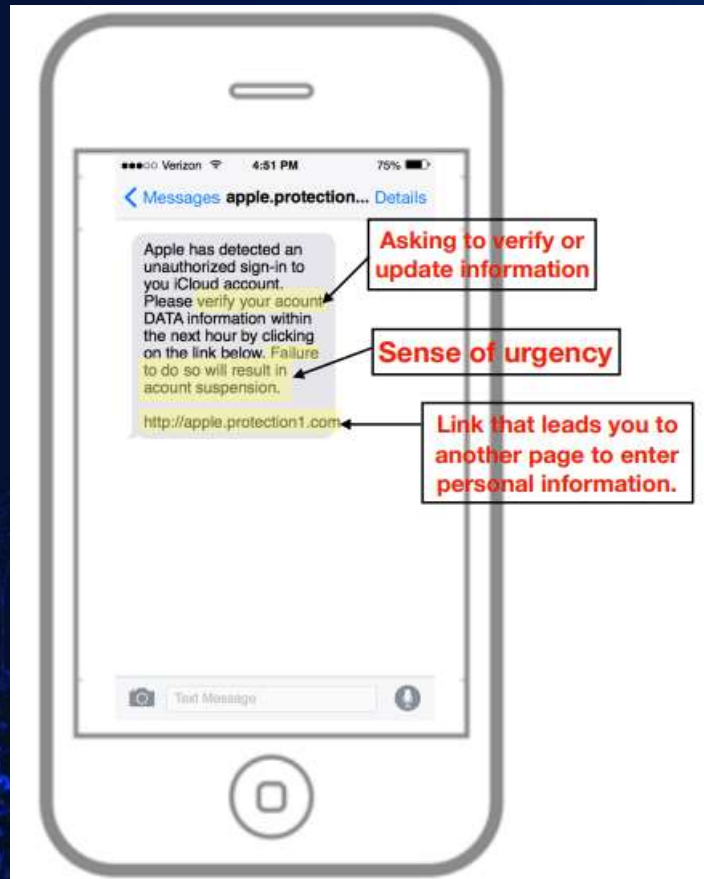
<https://en.wikipedia.org/wiki/Phishing>

Regards,
Mastercard IT

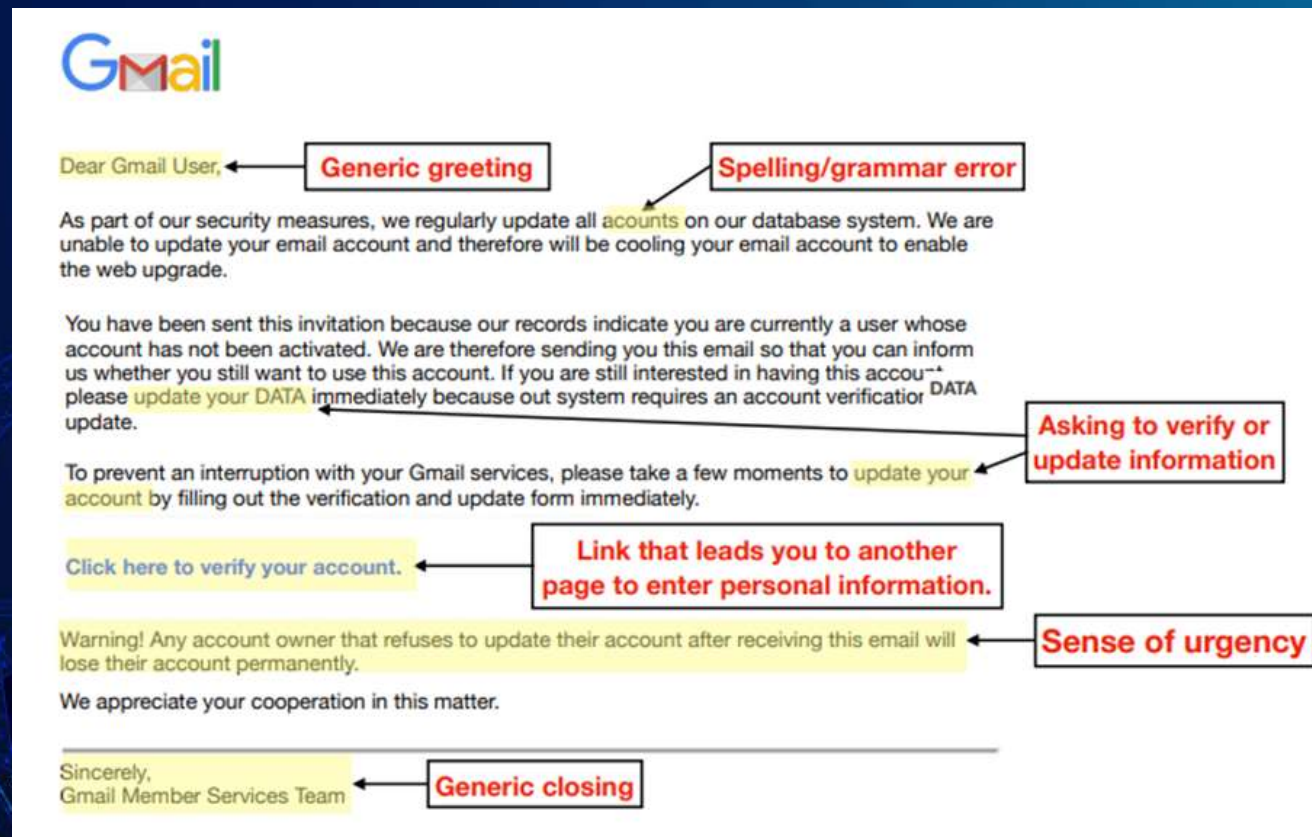
Recognizing & Avoiding phishing emails



Recognizing & Avoiding phishing emails



Recognizing & Avoiding phishing emails



Secure Your Devices from Phishing attacks

- Keep your anti-malware and anti-virus software up to date
- Don't use the same password for different accounts
- For critical accounts, use two-factor authentication
- Keep yourself informed about new cybersecurity risks



HOW DO WE STOP GETTING PHISHED?

- **Know what a phishing scam looks like**
- **Verify the sender by checking their email address** — WHO sender addresses use the person@who.int pattern. NOT Gmail, etc.
- **Check the link, before you click** — make sure the links start with https:// and not http://
- **Be careful when providing personal information** — never provide your credentials to third parties, not even the WHO.
- **Do not rush or panic react** — scammers use this in order to pressure you into clicking links or opening attachments.
- **If you gave sensitive information, don't panic** — reset your credentials on sites you've used them. Change your passwords and contact your bank immediately.
- **Report all scams.**