Phishing Awareness

Think Before You Click

CODE ALPHA

Introduction

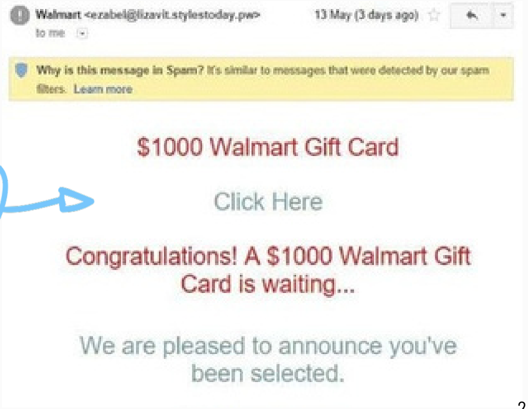
- Phishing is a cyber-attack technique
- Involves exploiting human psychology to extract sensitive information
- Using fake emails, messages, or fraudulent website

⚠ **Be aware and Avoid being the next victim**

Common Types Of Phishing Attacks

1. Email Phishing

DO NOT ! That’s obviously
a malicious link



Walmart <ezabel@lizavit.stylestoday.pw> 13 May (3 days ago)

to me

Why is this message in Spam? It's similar to messages that were detected by our spam filters. Learn more

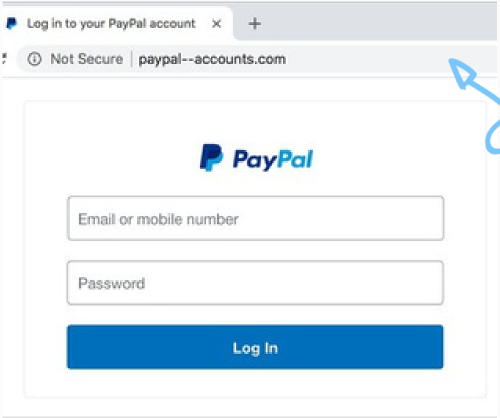
$1000 Walmart Gift Card

Click Here

Congratulations! A $1000 Walmart Gift Card is waiting...

We are pleased to announce you've been selected.

Common Types Of Phishing Attacks



Log in to your PayPal account ×

ⓘ Not Secure | paypal--accounts.com

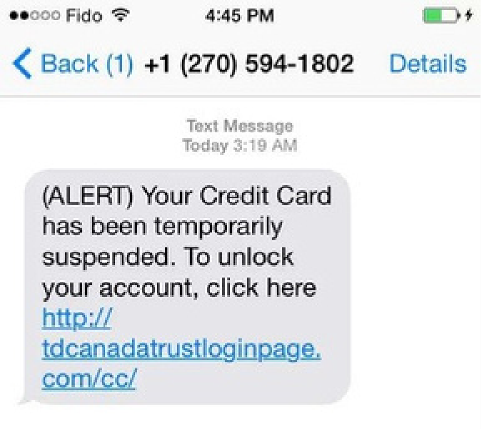
2. Website Phishing

Alert! Unsecure page Not the official PayPal website Do not enter your credentials

Common Types Of Phishing Attacks

Spam message !
DO NOT CLICK

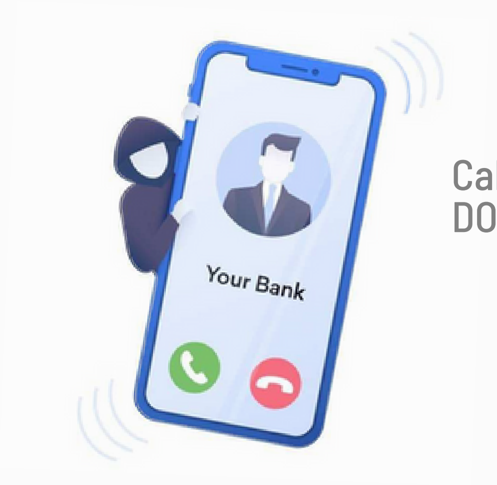
3. Smishing (SMS Phishing



Text Message
Today 3:19 AM

(ALERT) Your Credit Card has been temporarily suspended. To unlock your account, click here http://tdcanadatrustloginpage.com/cc/

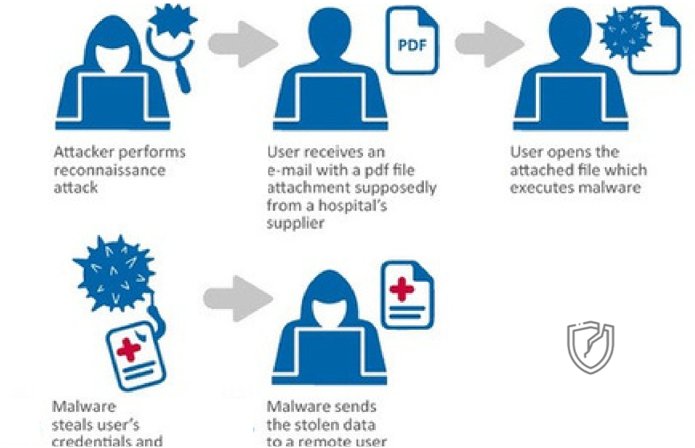
Common Types Of Phishing Attacks



Caller ID Spoofing
DO NOT FALL

4. Vishing (Voice Phishing)

Scenario Of A Social Engineering Attack



Attacker performs reconnaissance attack

User receives an e-mail with a pdf file attachment supposedly from a hospital's supplier

User opens the attached file which executes malware

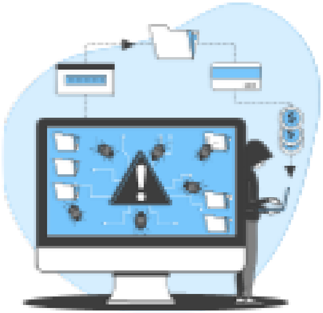
Malware steals user's credentials and

Malware sends the stolen data to a remote user

Detecting An Attempt Of Phishing Email

- Check the sender's email adress
- Inspect the Email Content
- Examine Links Before Clicking
- Verify Unexpected Password Reset Emails
- Avoid Opening Suspicious Attachments

Detecting An Attempt Of Phishing Website



- ☑ Use Anti-Phishing Software
- Check the Website URL
- Look for HTTPS
- ✓ Verify the Website’s Legitimacy
- ⊘ Be Skeptical of Pop-Up Windows

Safety Protocols To Avoid Phishing

- Patch and Update security softwares
- Train and Educate Employees
- Use Two-Factor Authentication (2FA)
- Report Suspicious Attempts

Thanks!