

DON'T GET HOOKED

How to Recognize and Avoid

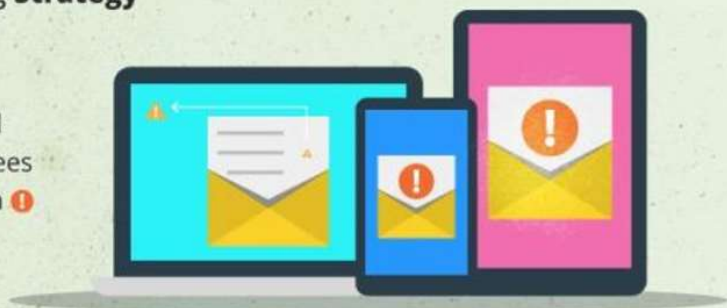
PHISHING ATTACKS



What is Phishing?

► The Go-To Social Engineering **Strategy**

Phishing attacks are **techniques** used by cybercriminals to con users/employees into **revealing sensitive information** ⓘ or **installing malware** ⚠ by way of electronic communication.



Phishing Attack Methods

MOST COMMON
TYPE OF
PHISHING
ATTACK

MASS-SCALE PHISHING

Attack where fraudsters **cast a wide net of attacks** that aren't highly targeted

HIGHLY TARGETED
TYPE OF
PHISHING
ATTACK


SPEAR PHISHING

Tailored to a **specific victim or group of victims** using personal details

THE MOBY DICK
OF PHISHING
ATTACKS

WHALING

Specialized type of spear phishing that **targets a "big" victim** within a company e.g., CEO, CFO, or other executive



Keep Your Eyes Peeled for **All Forms** of Phishing Attacks

EMAIL PHISHING

Fraudsters send **phony emails** that appear to come from valid sources in an **attempt to trick users** into revealing personal and financial information

What to look for?

The image shows a screenshot of an email client interface with several red boxes and lines pointing to specific elements, each labeled with a red box containing a warning sign. The email header shows 'From: EasyPay Support' (labeled 'Sender Name and Domain Spoof Known Brand'), 'To: AP@yourcompany.com', and 'Subject: Please pay overdue toll'. The message body contains a 'Notice to Appear,' (labeled 'Impersonalized Messages'), a typo 'paied' (labeled 'Grammatical Errors'), and a sentence 'The fee is past due.' (labeled 'Scare Tactics'). The signature is 'John Doe, EasyPass Agent' (labeled 'Imitating a Known Brand'). An attachment 'E-ZPass_0000300019.zip' is shown (labeled 'Compressed Attachments (e.g., zip files)').

From: EasyPay Support
To: AP@yourcompany.com
Cc:
Subject: Please pay overdue toll

Message: E-ZPass_0000300019.zip

Notice to Appear, Impersonalized Messages

You have not paied for driving on a toll road and the fee is past due. Grammatical Errors

The copy of the invoice is attached to this email.

Best Regards,
John Doe
EasyPass Agent Imitating a Known Brand

Scare Tactics

Compressed Attachments (e.g., zip files)

E-ZPass_0000300019.zip

Highly Personalized Messages

Unlike mass phishing emails, spear phishing messages are highly personalized and will often reference coworkers' or friends' names

To: jsmith@bigbank.com

Subject: Urgent Notice

Dear James,

We were contracted by your HR Director, Anne Wallace.

Embedded Malicious Files

Common file attachments (.doc, .xls, .ppt, etc.) can contain malicious macros



Security Warning Macros have been disabled.

Enable Content

Spoofed Links

Spoofed link text can hide a hyperlink's actual destination

To: jsmith@bigbank.com

Subject: Urgent Notice

http://69.195.85.136/~wrER3/sper323.html

<https://www.bankofamerica.com>

Spoofed Websites

Links to spoofed versions of well-known websites can look legitimate and are used to steal info submitted via forms or distribute malware to visitors

<https://www.bankofamerica.com>

Secure Sign-In

Banking

Credit Cards

VISHING

Short for "**voice phishing**," vishers use the telephone to solicit unsuspecting victims for **financial or personal details**

What to look for?

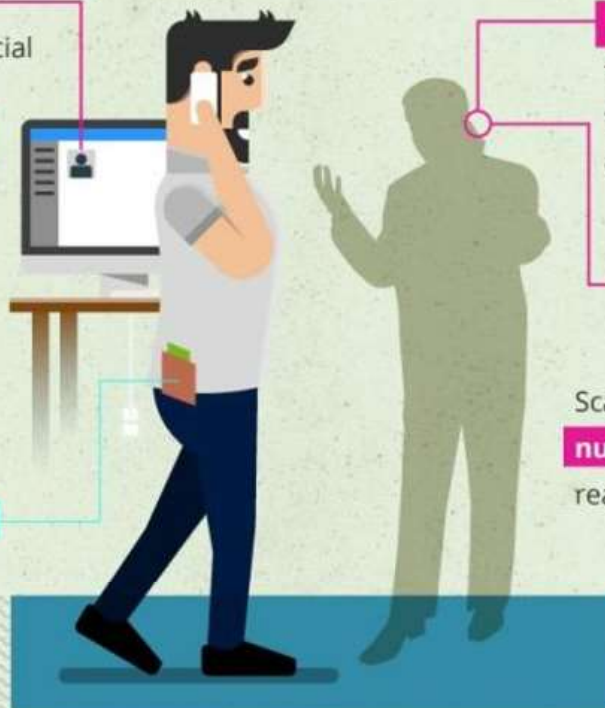
Personal data

can be gathered from social media profiles, providing criminals with **sensitive details** to make attacks seem more legitimate

Vishers utilize

fear tactics

to con you into thinking **your money is in danger** and you must act quickly



Persuasive phone tactics

that are **too good to be true** are a dead giveaway of criminal activity

Phoenix, AZ
555-555-5555

Scammers often **alter phone number/IDs** to disguise the real origin of the call



Vishers are posing as **IRS Agents**



Threatening parties with police arrest, deportation, license revocation, etc.

IRS reports from January 2016 show that since October 2013:



896,000

people have been **solicited** by scammers **claiming to be IRS officials**

5,000

VICTIMS HAVE COLLECTIVELY

PAID OVER

\$26.5 MILLION

AS A RESULT

SMISHING

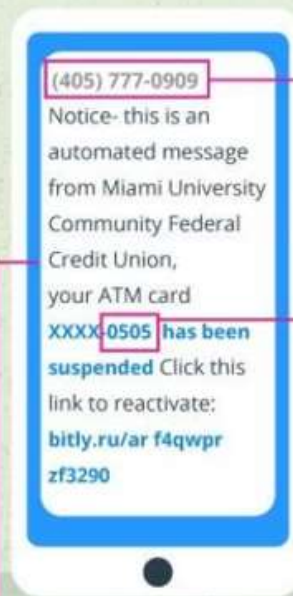
SMS messaging attacks where fraudsters send phony texts in an attempt to con you into **divulging private information** or **infecting your phone with malware**

What to look for?

"5000" or other non-cell numbers

are most likely scammers **masking their identity** by using email to text services

Texts can direct you to **spoofed websites** that **impersonate** your accounts and **attempt to infect** your phone with malware or **steal** information



Alarm bells should ring in your head when you receive texts from **unknown numbers** or **unsolicited messages**

Smishers may use the **first few digits** of your debit/credit card to pressure a response

Banks, financial institutions, social media platforms, and other business accounts should be contacted directly to determine if they sent you a legitimate SMS request

SMISHERS HAVE EVEN SPOOFED TWO FACTOR AUTHENTICATION FOR GMAIL, HOTMAIL, AND YAHOO MAIL

Authentication systems were breached by "smishers" who conned users into resetting their passwords in order to gain access to victims' email accounts



Attacker secures a victim's **email address / phone number** from public sources



Attacker **poses as the victim** and asks Google for a **password reset**



Google **sends a reset code** to the victim



SOCIAL MEDIA PHISHING

Cybercriminals use social media as a channel to carry out phishing attacks aimed at stealing personal information or spreading malware; some attacks are even used to hijack your accounts to launch follow-up attacks on your connections or followers

What to look for?

Playing Pretend

Scammers create replica accounts and inform victim's friends/followers that their previous account was abandoned

Messages are sent to victim's friends that demand the recipient to click on a link with an aim to collect personal data, e.g. credit/debit card numbers



Ray Thomas
30 mins
Decided to make a new account!
Like Comment Share

Bogus Posts

Social network feeds can contain bogus posts that trick users into clicking on a link and providing personal info



Register now for free a membership

Social Media Malware

Scammers can pose as a friend/follower and send messages with links to sites that are infected with malware

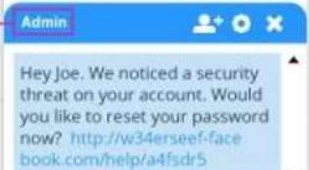
Even messages from known friends and followers may include links to sites that have been hacked



Ray Thomas
30 mins
Hey check this out, i can't believe they got this picture of you!! bit.ly.xyz/345Fw04
Like Comment Share



Ray Thomas
Hey Joe. You should sign up for this free giveaway. <http://w34erseef-face-book.com/help/a4fsdr5>



Admin
Hey Joe. We noticed a security threat on your account. Would you like to reset your password now? <http://w34erseef-face-book.com/help/a4fsdr5>

Stay Suspicious

Phishers can pose as admins from social networking sites in an effort to gain access to passwords/other account info

First Things First—Be Vigilant Online and Use Your Common Sense!



Always be suspicious of any unsolicited communication from businesses or individuals, regardless of the message medium

Don't click on links or attachments in suspect emails, texts, or social media messages

Directly contact the purported sender via their official website, phone number, or email address if you are not sure about the legitimacy of a message you have received

Report suspected phishing scams to your IT and security teams

File a complaint with the FBI Crime Complaint Center (IC3) to help shut down cybercriminals