

DON'T GET HOOKED

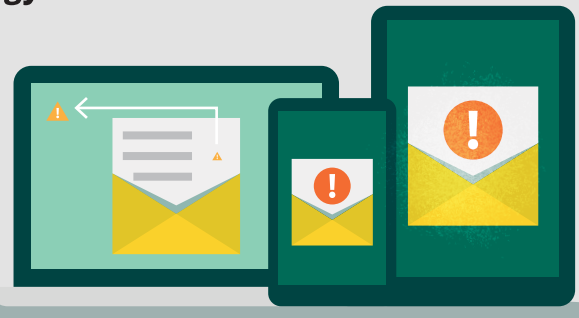
How to Recognize and Avoid PHISHING ATTACKS



What is Phishing?

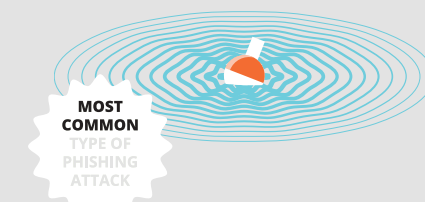
The Go-To Social Engineering Strategy

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



Keep Your Eyes Peeled for All Forms of Phishing Attacks

Phishing Attack Methods



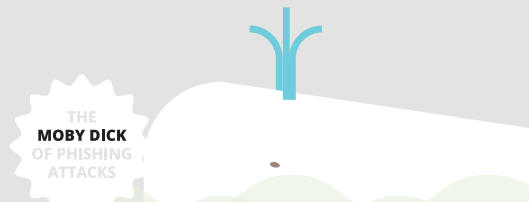
MASS-SCALE PHISHING

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



SPEAR PHISHING

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



WHALING

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

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?

Sender Name and Domain Spoof Known Brand
From: EasyPay Support
To: AP@yourcompany.com
Subject: Please pay overdue toll

Compressed Attachments (e.g., zip files)
E-ZPass_0000300019.zip

Impersonalized Messages
Notice to Appear, Impersonalized Messages

Grammatical Errors
You have not paid for driving on a toll road and the fee is past due. The copy of the invoice is attached to this email.

Scare Tactics
Best Regards, John Doe, EasyPass Agent

Imitating a Known Brand

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
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

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

5000
Dear Walmart shopper, Congratulations you have just won a \$1000 Walmart Gift Card. Click here to claim your gift.
www.WalmartClick.com (cancel reply STOP)

(405) 777-0909
Notice: this is an automated message from Miami University Community Federal Credit Union, your ATM card XXXX0505 has been suspended. Click this link to reactivate: bitly.ru/ar4qwpz3f3290

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

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

Smishers may use the last 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

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

Bogus Posts

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

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
Decided to make a new account

Register now for free a membership

Ray Thomas 30 mins
Hey check this out, I can't believe they got this picture of you! bitly.xyz/345Fw04

Ray Thomas 30 mins
Hey Joe, You should sign up for this free giveaway http://w34erseeef-face-book.com/help/a4f5d5

Admin
Hey Joe, We noticed a security threat on your account. Would you like to reset your password now? http://w34erseeef-face-book.com/help/a4f5d5

Stay Suspicious

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

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:



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

Authentication systems were breached by "smishers" who coned 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
- Smisher texts victim with fraudulent message: "Google has detected unusual activity on your account. Please respond with the code sent to your mobile device immediately."
- Victim sends the password verification code to the smisher thinking that the request came from Google
- Attacker uses the code to reset the victim's password and take control of their account

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

Sources
security.intuit.com/phishing.html
bbc.com/news/business-35201188
ic3.gov/media/2015/1/150827-1.aspx
resources.infosecinstitute.com/the-most-popular-social-network-phishing-schemes
digitalguardian.com/blog/social-engineering-attacks-common-techniques-how-prevent-attack
networkworld.com/article/2978137/security/fbi-major-business-e-mail-scams-blasts-270-increase-since-2015.html
money.usnews.com/money/personal-finance/articles/2013/09/19/how-to-protect-yourself-from-smishing-and-vishing?page=2
networkworld.com/article/2164211/infrastructure-management/how-to-avoid-becoming-a-victim-of-smishing-sms-phishing.html
irs.gov/uac/newsroom/phone-scams-continue-to-be-a-serious-threat-remain-on-irs-dirty-dozen-list-of-tax-scams-for-the-2016-filing-season

FORTRA
Digital Guardian

DEVELOPED BY
NEWSOURCING