

DON'T GET HOOKED

How to recognise and avoid Phishing Attacks

What is Phishing?

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



Email Phishing

Fraudsters send fake 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,

Grammatical Errors

You have not paied 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

Embedded Malicious Files

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

Spoofed Links

Spoofed link text can hide a hyperlink's actual destination

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

To: jsmith@bigbank.com

Subject: Urgent Notice

Dear James,

We were contracted by your HR Director, Anne Wallace.

Security Warning: Macros have been disabled. Enable Content

To: jsmith@bigbank.com

Subject: Urgent Notice

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

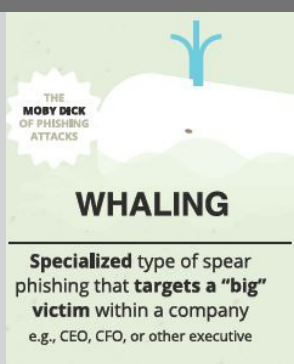
https://www.bankofamerica.com

https://www.bankofannerica.com

Secure Sign-In

Banking Credit Cards

Keep your eyes peeled for all forms of Phishing attacks



Smishing

SMS messaging attacks where fraudsters send fake texts in an attempt to get you into divulging private information or infecting your phone with malware (viruses)

What to look for?

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 **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 Smishing

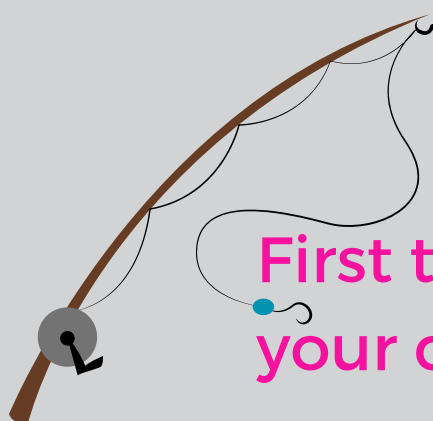
What to look for?

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

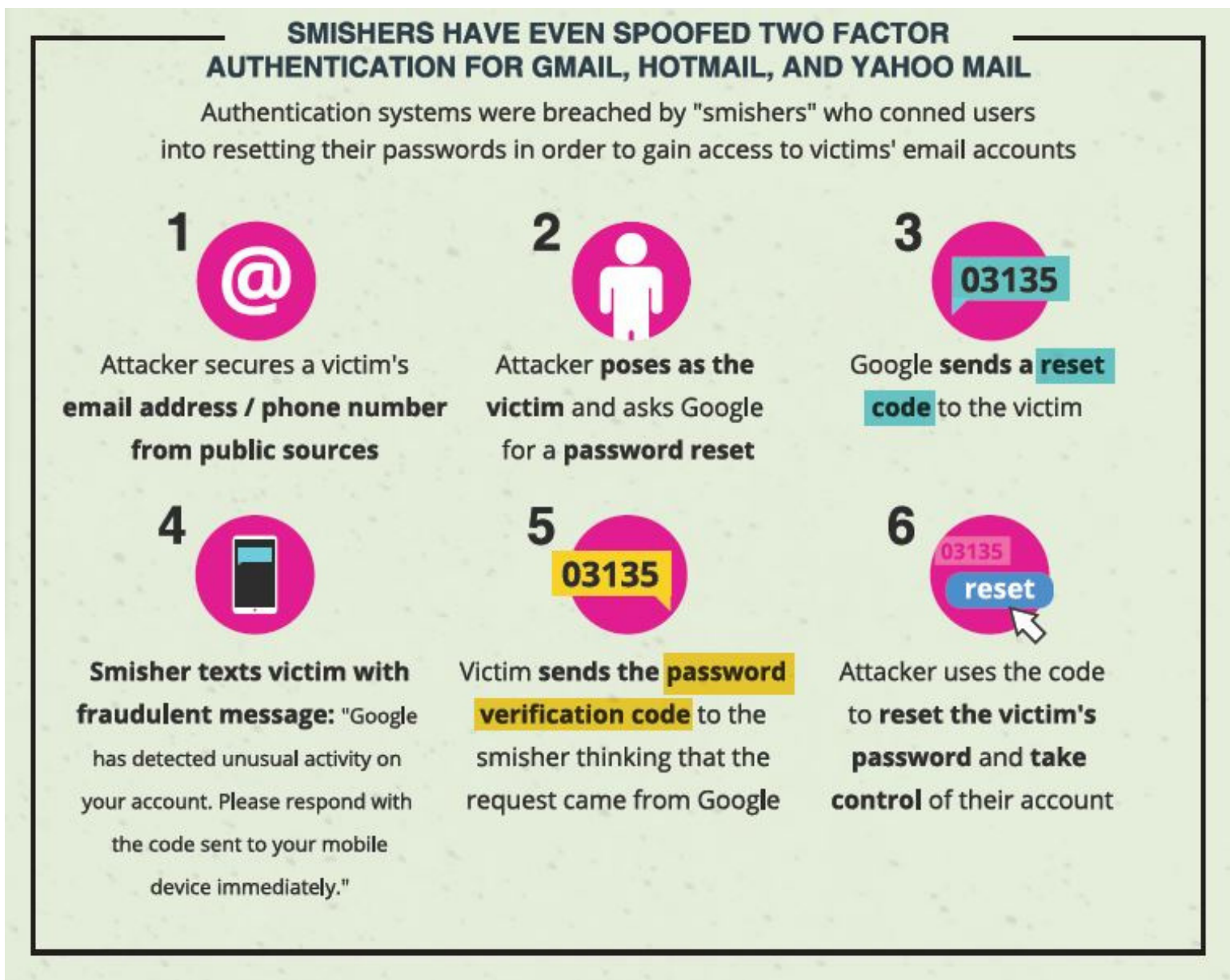
Bogus Posts
Social network feeds can contain bogus posts that trick users into clicking on a link and providing personal info

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

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



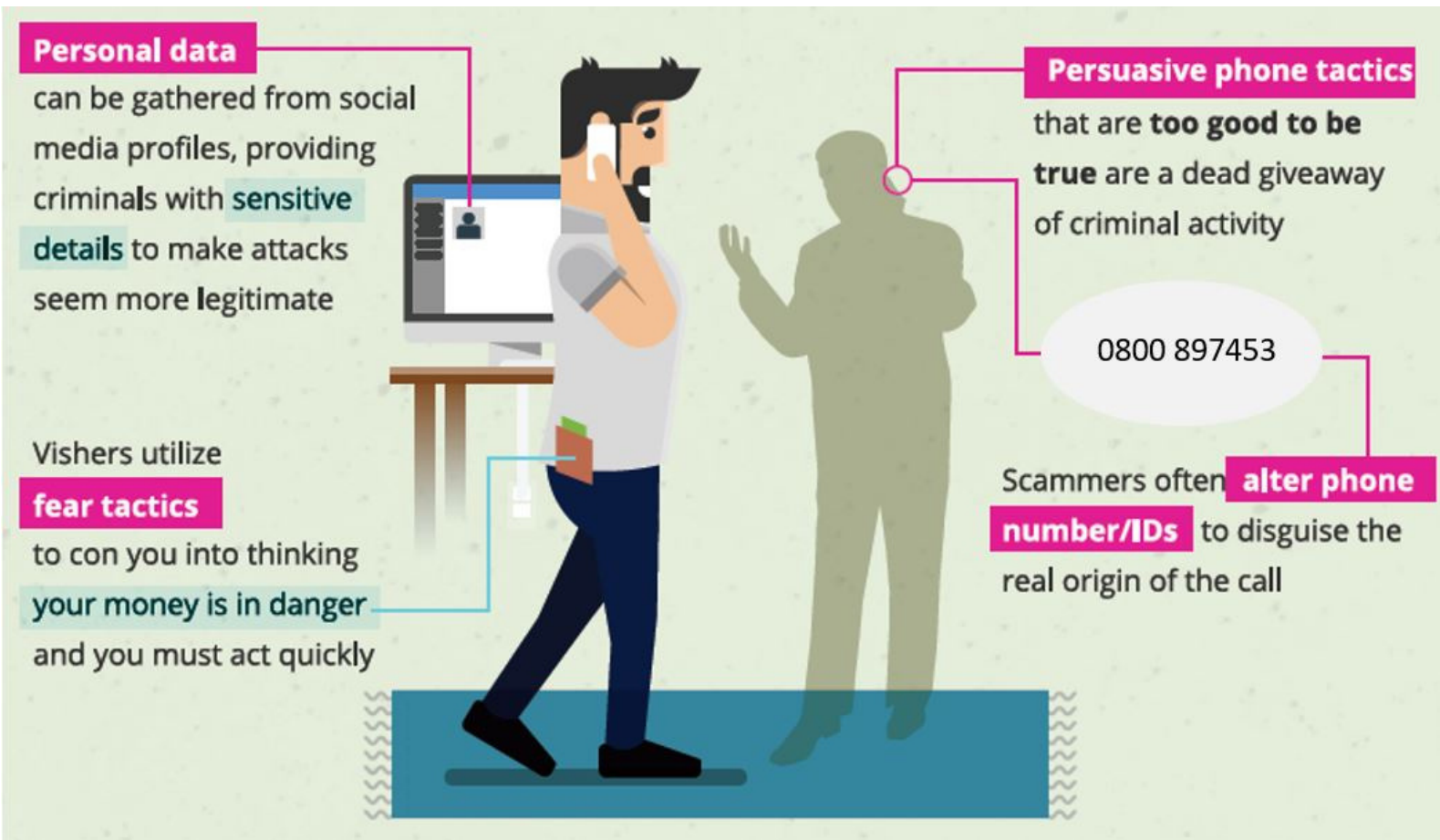
First things first - Be vigilant and use your common sense! Don't get hooked!



Vishing

Short for 'voice phishing', vishers use the phone to solicit unsuspecting victims for financial or personal details

What to look for?



Always be suspicious of any unsolicited communication from businesses or individuals

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

Report suspected phishing scams to your IT team