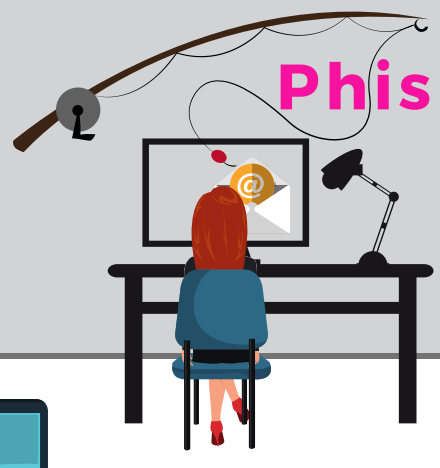
DON'T GET HOOKED

How to recognise and avoid Phishing Attacks

What is Phishing?

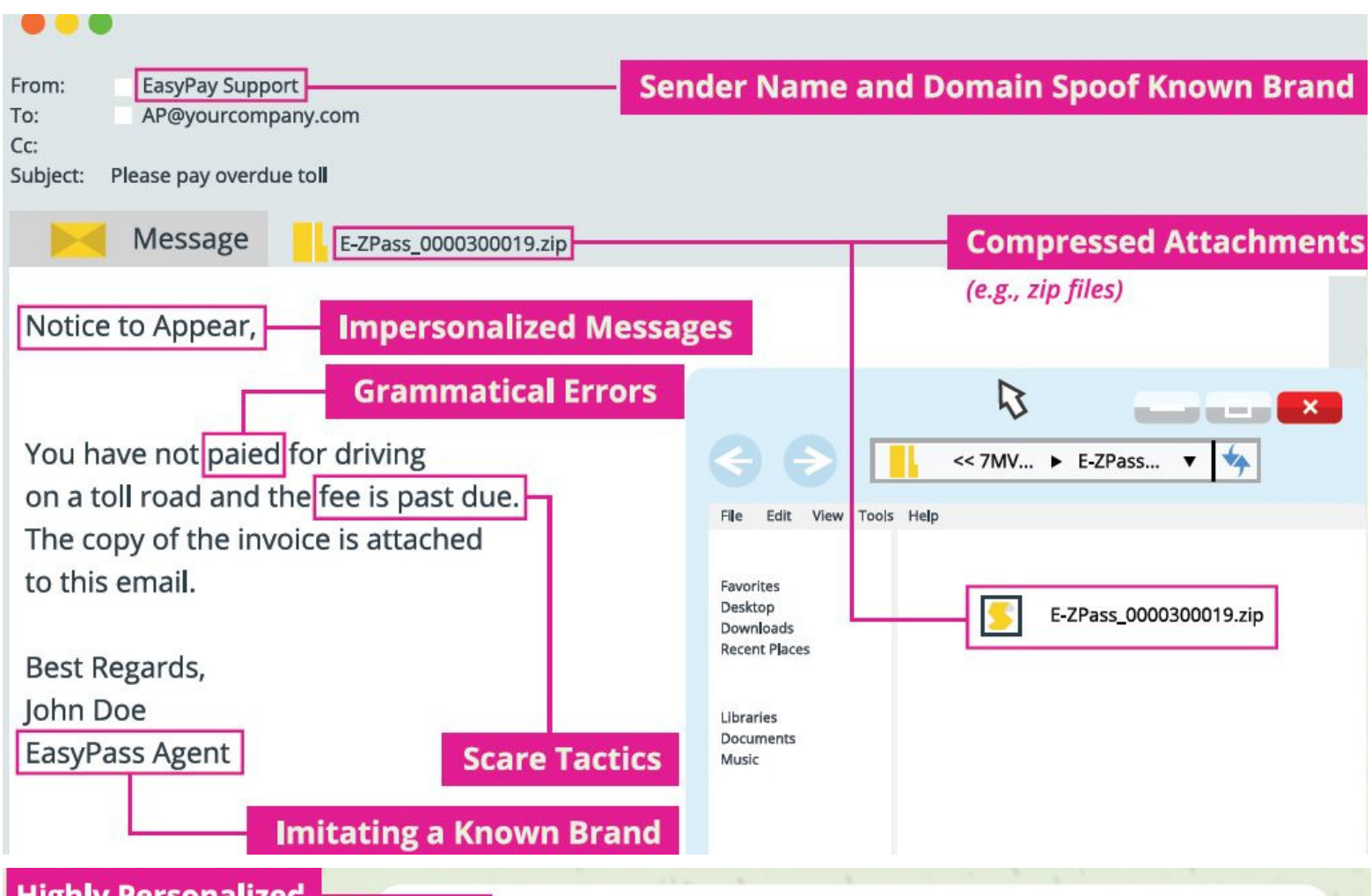
Phishing attacks are techniques used by cyber criminals to con users/employees into revealing sensitive information or installing malware by way of electronic communication



Email Phishing

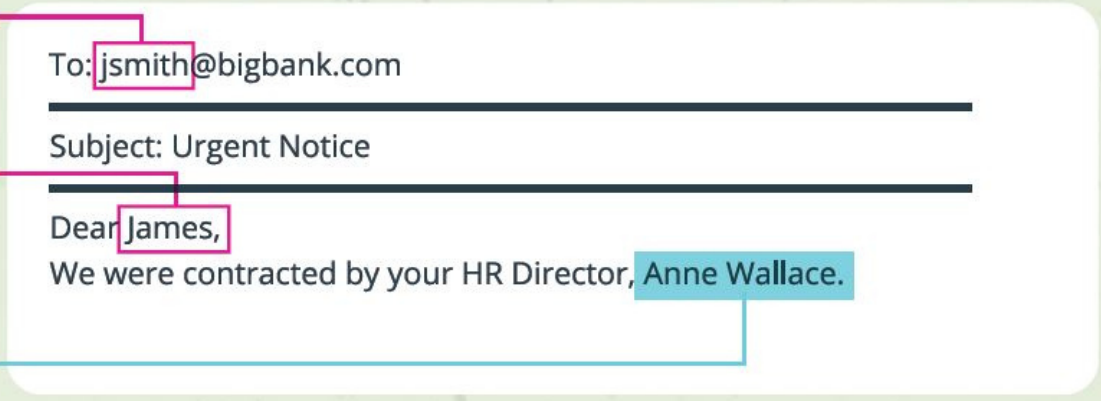
Fraudsters send fake emails that appear to come from valid sources in an attempt to trick users into revealing personal and financial information

What to look for?



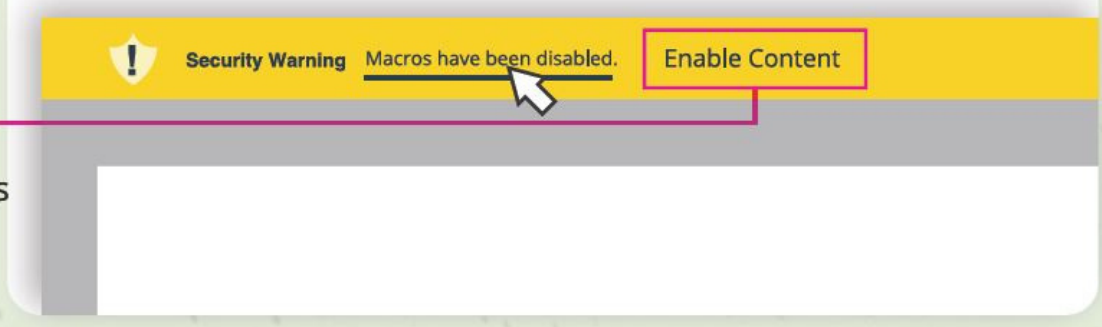
Highly Personalized Messages

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

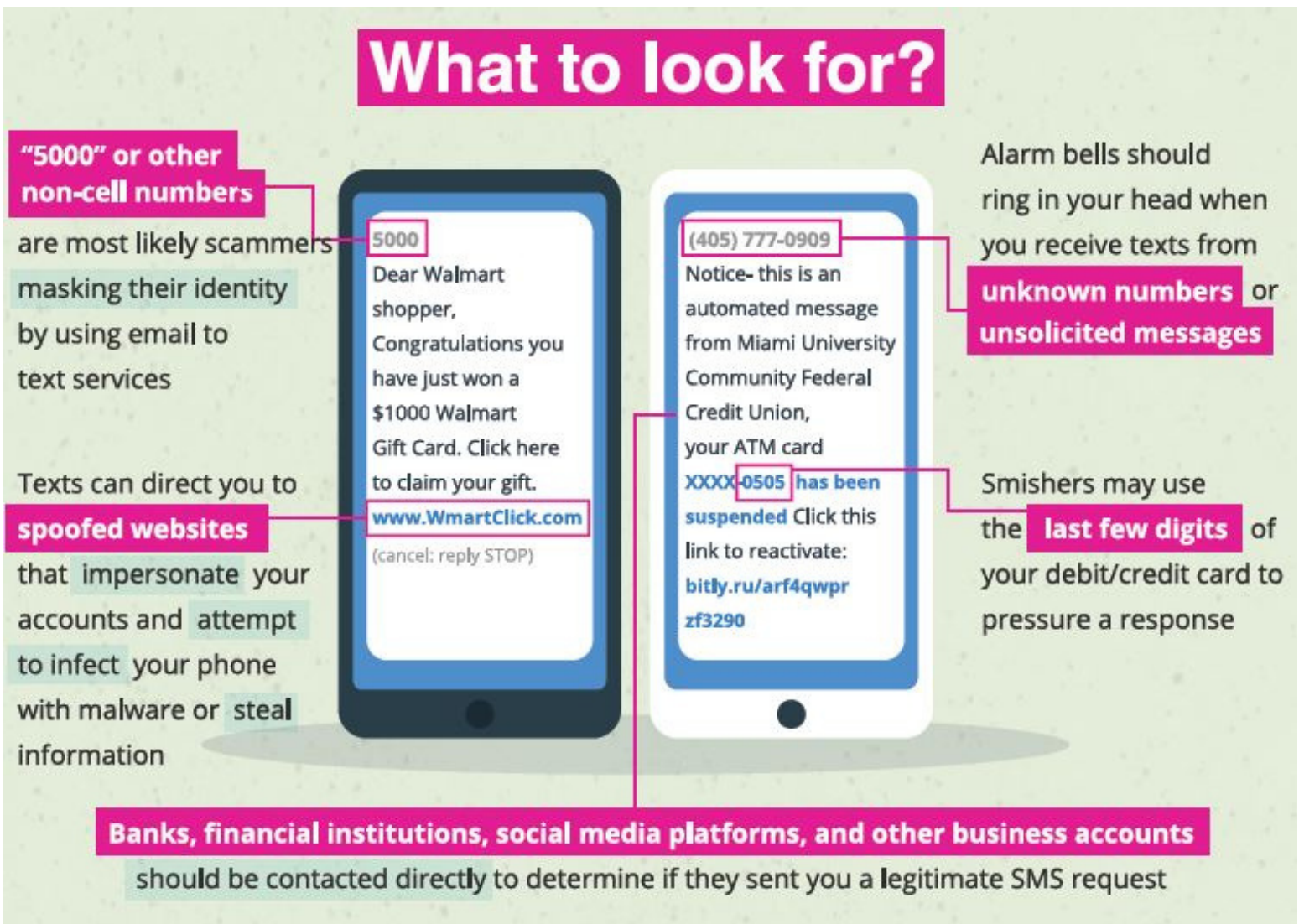
Links to spoofed versions of well-known websites can look legitimate and are used to steal info submitted via forms or distribute malware to visitors

Keep your eyes peeled for all forms of Phishing attacks

Smishing

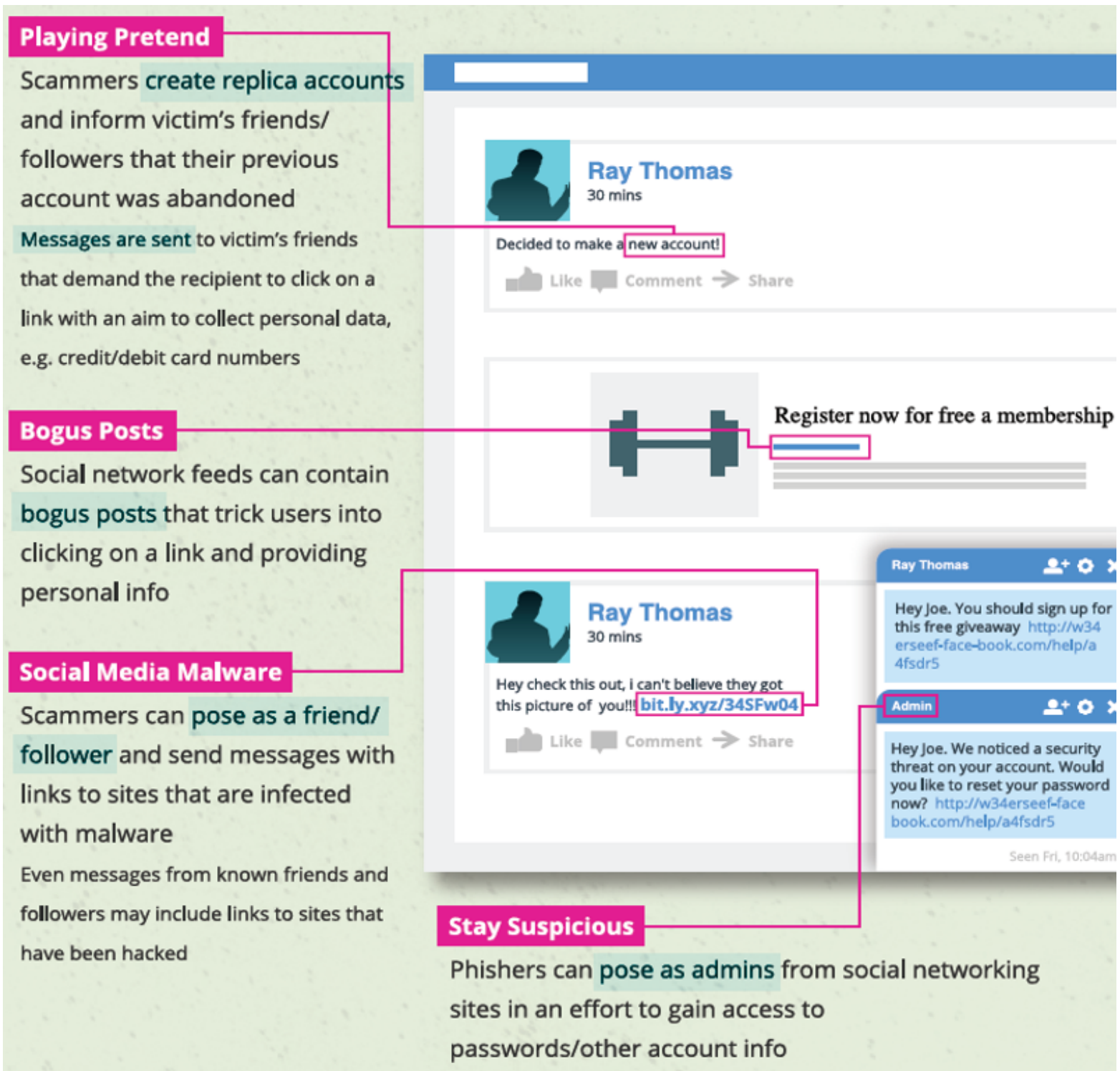
SMS mesaging attacks where fraudsters send fake texts in an attempt you into divulging private information or infecting your phone with malware(vriuses)

What to look for?

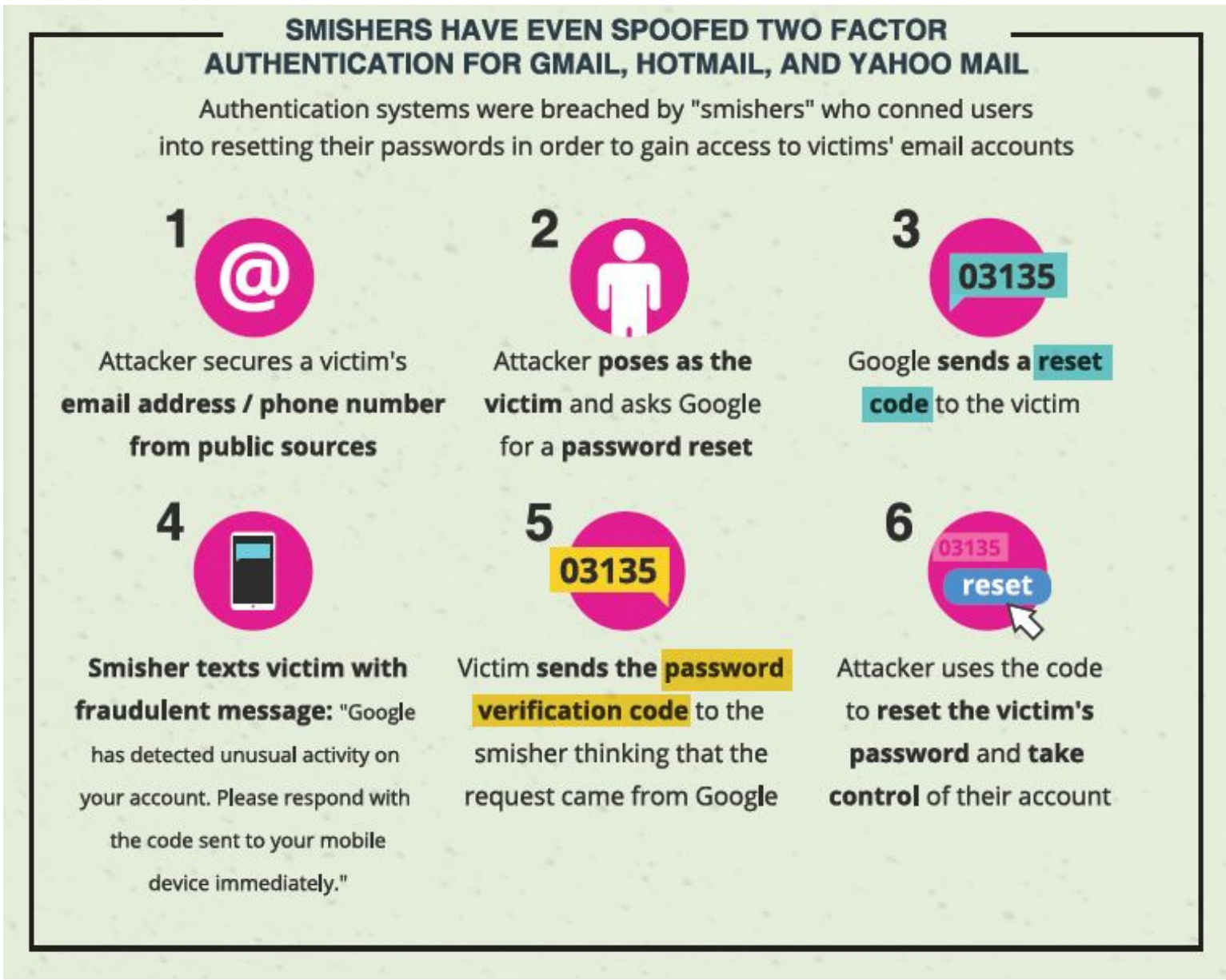


Social Media Smishing

What to look for?



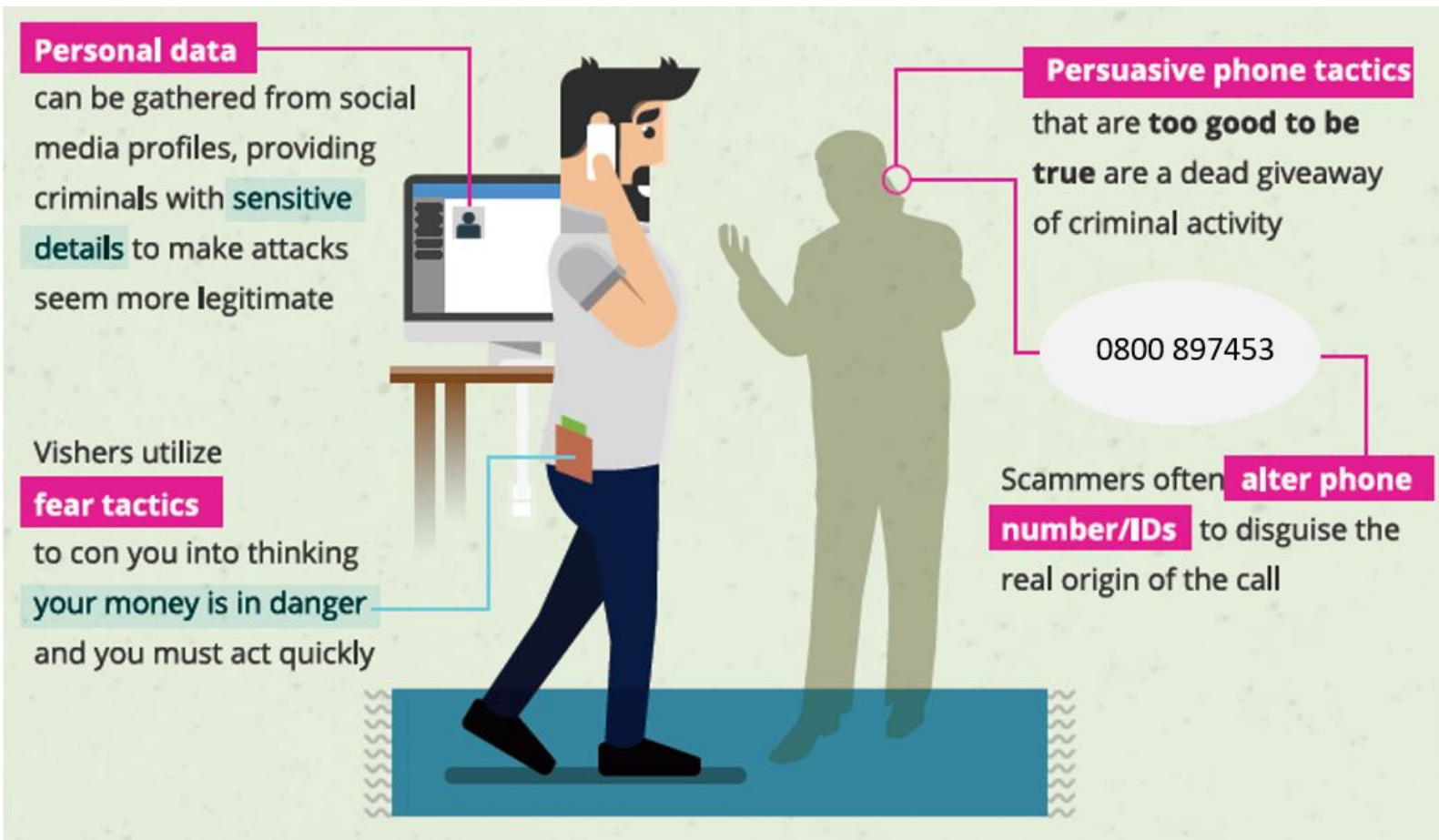
First things first - Be vigilant and use your common sense! Don't get hooked!



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 unsolicitored communication from businesses or individuals

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

Report suspected phishing scams to your IT team

An information leaflet produced by

L.E.A.D. IT Services
Lead · Empower · Achieve · Drive

01332 861956

ictsupport@leaditservices.co.uk