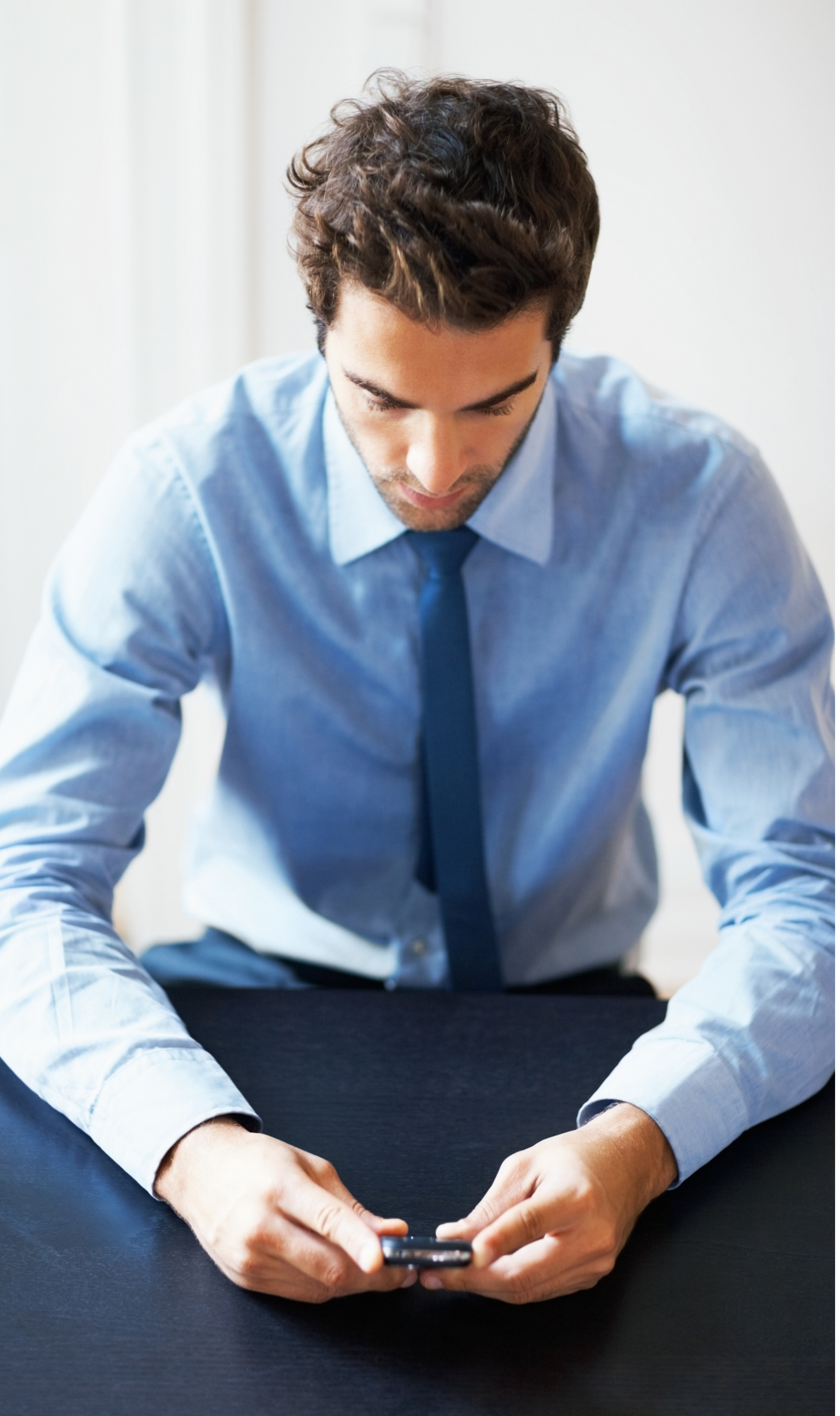
Ntiva

Your Success. Secured.

SMISHING: YOUR GUIDE TO SMS PHISHING

A SECURITY AWARENESS USER GUIDE



SO...WHAT *EXACTLY* IS SMISHING?

Smishing is SMS-phishing.

Smishing is the term that many in the security industry are using to describe a social engineering technique that exploits its victims using SMS, or text messaging. Where phishing uses email as the entry point of attack, Smishing, (sometimes called "SMiShing") uses text messages as its point of entry.

Smishing is a relatively new trend, and one that is particularly alarming.

Most of us are aware of the phishing threat around our email inboxes and therefore, tend to exercise caution.

But many of us *aren't* aware of the threat that's presented in our cell phone's text message inbox and therefore, we tend to trust text messages more than we do emails, even from unknown senders.

This elevates the probability that we will click on a malicious item sent to us via text.

Hackers know this too, and that's why they're using Smishing attacks at an increasing rate.

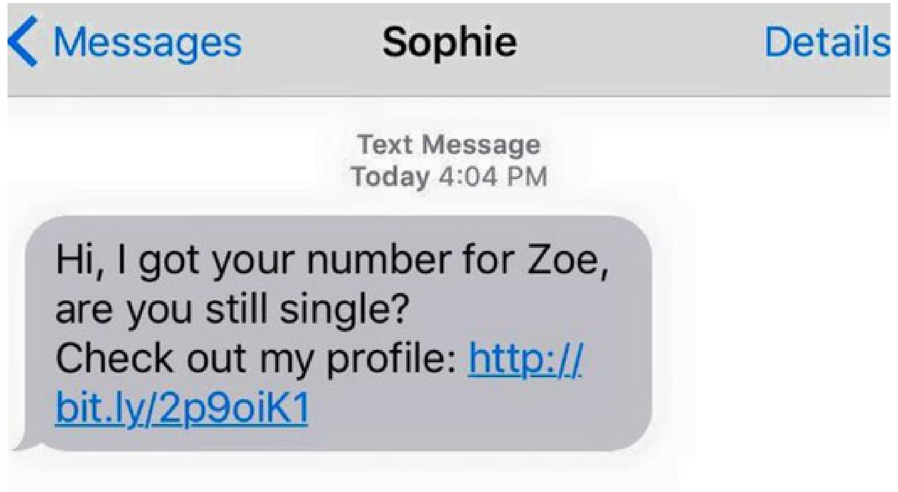
WHAT DOES A SMISHING MESSAGE LOOK LIKE?

It's common to receive a Smishing message that alerts you to daily charges that you will begin receiving unless you opt-out of the service.

A link will be provided and you will be instructed to follow that link in order to opt-out of the service and avoid daily charges.

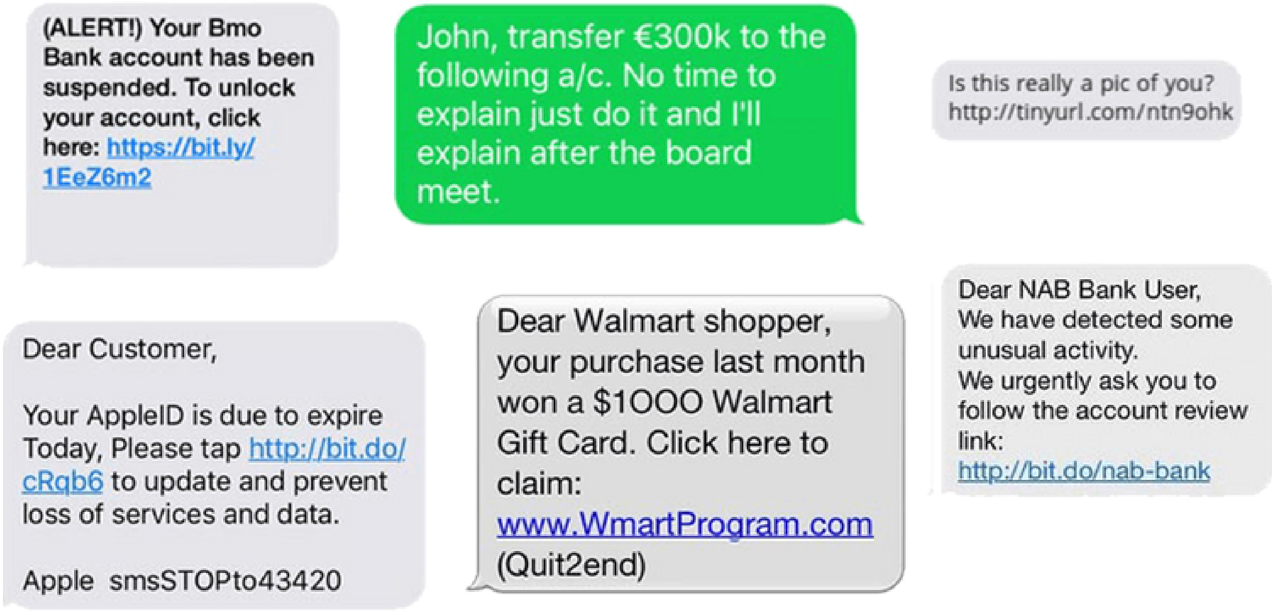
When you click the link, you're brought to a website page that asks you to fill out a form if you want to opt-out of the service. The form will ask for your personal information.

If you submit this information, the person behind the scam will either keep your information to use in other fraudulent acts or they will sell it on the dark web to other criminals in the market for stolen identities.



Text Message
Today 4:04 PM

Hi, I got your number for Zoe, are you still single?
Check out my profile: http://bit.ly/2p9oiK1



(ALERT!) Your Bmo Bank account has been suspended. To unlock your account, click here: https://bit.ly/1EeZ6m2

John, transfer €300k to the following a/c. No time to explain just do it and I'll explain after the board meet.

Is this really a pic of you? http://tinyurl.com/ntn9ohk

Dear Customer,

Your AppleID is due to expire Today, Please tap http://bit.do/cRqb6 to update and prevent loss of services and data.

Apple smsSTOPto43420

Dear Walmart shopper, your purchase last month won a $1OOO Walmart Gift Card. Click here to claim: www.WmartProgram.com (Quit2end)

Dear NAB Bank User,
We have detected some unusual activity.
We urgently ask you to follow the account review link:
http://bit.do/nab-bank

SMISHING IS THE NEXT EVOLUTION IN DATA THEFT

While it may seem low-tech, a successful smishing attack can put everything inside your corporate network at risk. Think about how many individuals bring their own devices to your place of business. Cell phones are so prevalent that they have become a favorite method of bringing security hazards into the workplace environment. Just a single slip from a well-meaning accountant or an accidental click from a C-level can have a devastating impact on your place of business.

In fact, in the first six months of 2021...

SMISHING ATTACKS INCREASED 700%!

https://www.itpro.com/security/scams/360873/smishing-attacks-increase-700-percent-2021

HERE ARE THREE COMMON SMISHING SCAMS YOU NEED TO WATCH FOR:

BANK SMISHING

This scam tries to get you to act by saying your bank account has been hacked, when in reality, this is the hacking attempt itself. It usually starts with a text message claiming to be from your bank. This message is designed to alarm you, perhaps telling you that your security has been breached, that there’s been an abnormally large transfer, or a new payment recipient has been added to your account. It will then encourage you to click on a link, call a phone number, or reply with your PIN or login details. Under no circumstances should you follow any of these instructions or prompts. Instead, ignore the message and contact your bank to verify your account status.

MALWARE SMISHING

While not as common as bank smishing, malware smishing can be just as damaging. You may receive a text message encouraging you to download something onto your phone, like an app. This app may look like it’s from a trusted source, but it could be used to harvest sensitive data from your phone, like credit card details stored in other apps. These scams are commonplace over email, but have now been adapted for phones, too. Never download anything unless you are sure it’s from a trusted source.

MONEY SMISHING

In this case, fraudsters will try to persuade you to send someone money. It might look like a plea for money from someone you know, like a friend, colleague, or family member. It could also look like a text from an important organization, like a tax collector, insurance broker, church, or the police. For these scams, social engineering plays a huge role. They’ll try to make you feel panicked or guilty, so you’ll be tempted to send money quickly before you can identify it as a fraudulent request. By the time you’ve realized the truth, the scammer may have already accessed your accounts.

PROTECTING YOURSELF AGAINST SMISHING ATTACKS:

- ✓ **Never** click a reply link or phone number in a message you're not sure about.
- ✓ Treat "you-must-act-now" messages with great suspicion. This is a warning sign of a social engineering attempt.
- ✓ Financial institutions won't send you texts asking to update your account or confirm your card numbers. If you get a message like this that appears to be coming from your bank, don't click anything. Call your bank directly and report fraud.
- ✓ Look for suspicious numbers such as "5000" numbers. These numbers are tied to email-to-text services, which social engineers use to avoid using their personal phone numbers for the attacks.
- ✓ Protect your community, report all suspected smishing to the FCC to keep others safe from fraud.

Unfortunately, there's no fail-safe approach to total cyber protection. Investing in Security Awareness Training for your team is one of the best ways to accomplish your security goals.

READ THE BLOG

SECURITY AWARENESS TRAINING -- ARE YOU TRAINING YOUR TEAM TO RECOGNIZE CYBER THREATS?

Read Now