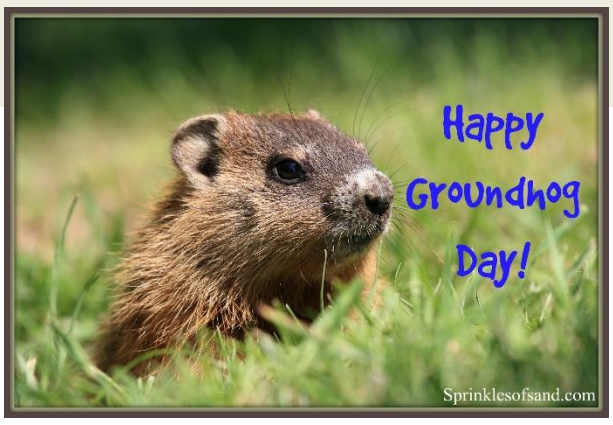
FEBRUARY 2, 2022 / / WEDNESDAY / / ISSUE 5

SECURITY NEWS

SCAM ALERTS AND HELPFUL TIPS

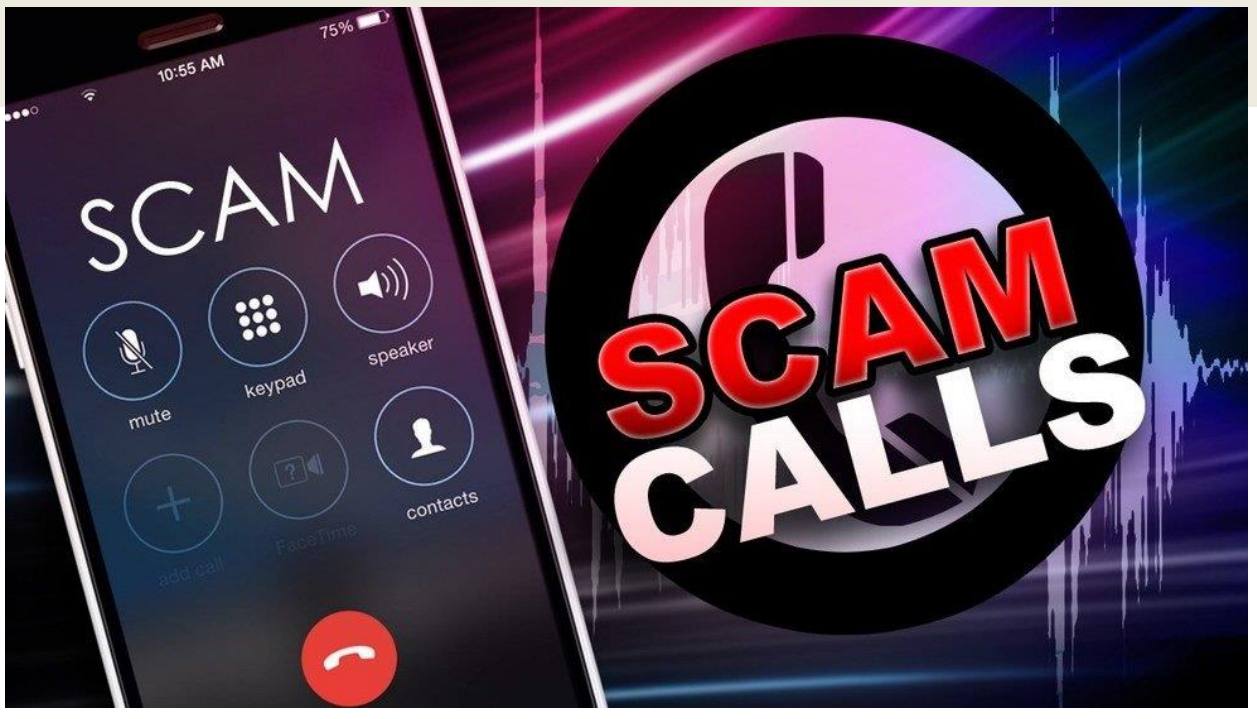


Hello February!!!

CHRIS MCDANIEL
FEBRUARY 2022

The Yadkin County Information Technology Department would like to wish everyone a Happy Groundhog Day. It is finally that time of year again when we find out if winter is going to stick around. Unfortunately Punxsutawney Phil saw his shadow this morning so we are in for six more weeks of this brutal cold weather. Hopefully spring temperatures will start coming around sooner. Just as a reminder the cold weather doesn't stop hackers and scammers from trying to steal your information so please stay security smart when working online.

The newsletter I have put together this month will focus on Scams that are being reported as well as tips to protect yourself from attackers. Please take some time to read over this month's article and tips. Remember there are cybercriminals out there constantly looking to ruin our lives and make things difficult. Let's not fall prey to their tricks and always remember to think before you click. Hope Everyone has a Happy Groundhog's Day and stays safe.



Beware of a New Google Vishing Scam

NCDIT
FEBRUARY 1, 2022

Vishing, or voice phishing, is the fraudulent practice of making phone calls or leaving voice messages purporting to be from reputable companies to induce individuals to reveal personal information, such as bank details and credit card numbers.

A new FBI advisory, "Building a Digital Defense Against Google Voice Authentication Scams," warns of a scam that is designed as a precursor to additional vishing scams and can perform Gmail account takeovers. The scam works even if you do not use Google Voice.

Google Voice is a service where Google provides users with a virtual phone number to make and receive calls and texts. The FBI advisory describes a scam that involves a threat actor who responds to a personal ad – they use the example of selling a couch on Craigslist or some other site – and says they want to make sure you are legitimate by sending you an authentication code from Google.

What is really happening is the scammer is setting up Google Voice using your phone number as the primary number and using you to assist them with Google's authentication process during setup. Once completed, the threat actor has a new Google Voice account tied to your mobile phone, so they can carry on without worrying about having it tied to their phone. Additionally, the code being sent could be used to allow them access to reset the password to your Google account.

Organizations relying on Gmail for corporate email should be specifically concerned about this scam. With Access to one of you internal email accounts, threat actors can easily send out phishing emails designed to gain access to devices or install ransomware.

The FBI offers the following advice to avoid getting scammed:

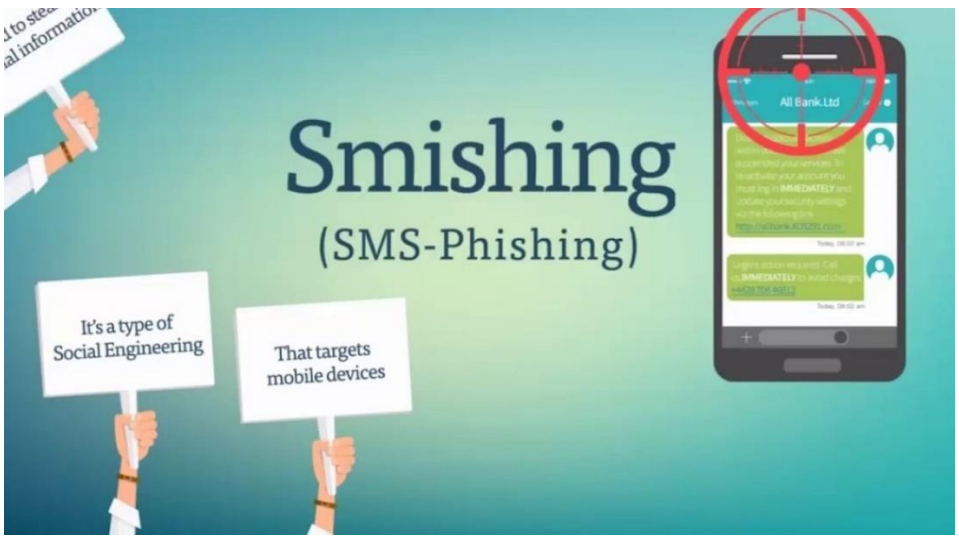
- Never share a Google verification code with others.
- Only deal with buyers and sellers in person. If you're exchanging money, make sure you are using legitimate payment processors.
- Do not give out your email address to buyers/sellers conducting business via phone.
- Do not let someone rush you into a sale. If they are pressuring you to respond, they are likely trying to manipulate you into acting without thinking.

To view the FBI advisory, click here. If you believe you are the victim of an online scam, report it to the FBI's Internet Crime Complaint Center at www.ic3.gov or call your local FBI office.

This article provided by the NCDIT may be found via the link provided here: NCDIT.

SPOT AND STOP MESSAGING ATTACKS

Jeff Lomas, SANS, January 5, 2022



What are messaging attacks?

Smishing (a consolidation word combining SMS and phishing) are attacks that occur when cyber attackers use SMS, texting, or similar messaging technologies to trick you into taking action you should not take. Perhaps they fool you into providing your credit card details, get you to call a number to get your banking information, or convince you to fill out an online survey to harvest your personal information. Just like in email phishing attacks, cyber criminals often play on your emotions to get you to act by creating a sense of urgency or curiosity, for example. However, what makes messaging attacks so dangerous is there is far less information and fewer clues in a text than there are in emails, making it extremely harder for you to detect that something is wrong.

A common scam is a message telling you that you have won an iPhone, and you only need to click a link and fill out the survey to claim it. In reality, there is no phone and the survey is designed to harvest your personal information. Another example would be a message stating that a package could not be delivered with a link to a website where you are asked to provide information needed to complete the delivery, including your credit card details to cover "service charges." In some cases, these sites may even ask to install an unauthorized mobile app that infects and takes over your device.

Sometimes cyber criminals will even combine phone and messaging attacks. For example, you may get and urgent text message from your bank asking if you authorized an odd payment. The message asks you to reply YES or NO to confirm the payment. If you respond, the cybercriminal now knows you are willing to engage and will call you pretending to be the bank's fraud department. They will then try to talk you out of your financial and credit card information, or even your bank account's login and password.

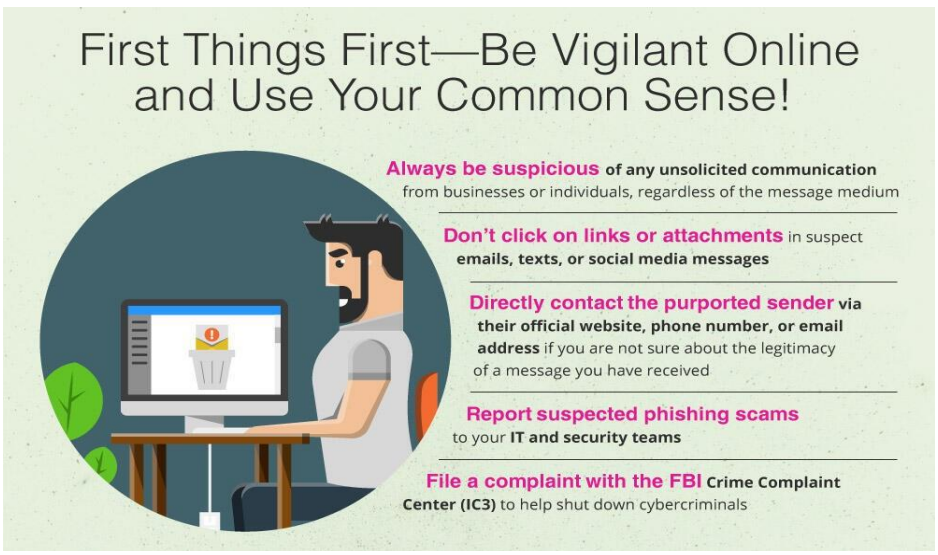
Spotting and Stopping Messaging Attacks

Here are some questions to ask yourself to spot the most common clues of a messaging attack:

- Does the message create a tremendous sense of urgency attempting to rush or pressure you into taking an action?
- Is the message taking you to websites that ask for your personal information, credit card, passwords, or other sensitive information they should not have access to?
- Does the message sound too good to be true? No, you did not really win a new iPhone for free.
- Does the linked website or service force you to pay using non-standard methods such as Bitcoin, gift cards or Western Union transfers?
- Does the message ask you for the multi-factor authentication code that was sent to your phone or generated by your banking app?
- Does the message look like the equivalent of a "wrong number?" If so, do not respond to it or attempt to contact the sender; just delete it.

If you get a message from an official organization that alarms you, call the organization back directly. Don't use the phone number included in the message, use a trusted phone number instead. For example, if you get a text message from your bank saying there is a problem with your account or credit card, get a trusted phone number on your bank's website, a billing statement, or from the back or you debit or credit card. Also remember that most government agencies, such as tax or law enforcement, will never contact you via text message, they will only contact you by old fashioned mail.

When it comes to messaging attacks, you are your own best defense.



The information for this article from SANS may be found via the link provided here: SANS OUCH! Newsletter.

VISHING

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

What to look for?

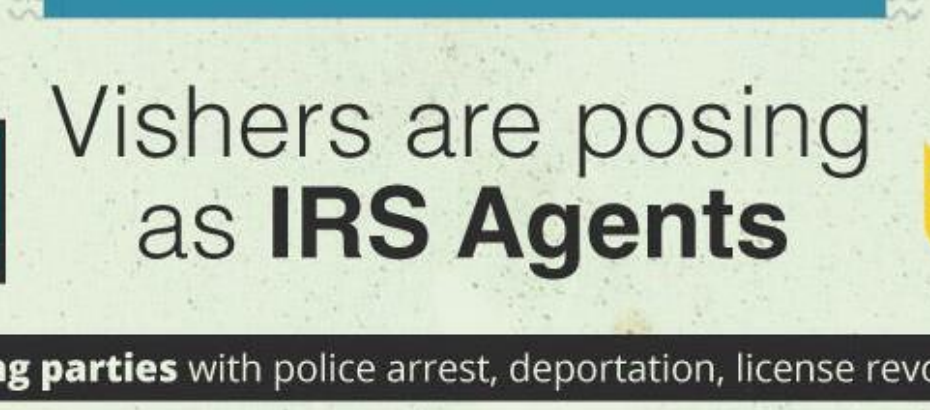
Personal data can be gathered from social media profiles, providing criminals with sensitive details to make attacks seem more legitimate

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

Phoenix, AZ
555-555-5555

Vishers utilize **fear tactics** to con you into thinking your money is in danger and you must act quickly

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

8 TIPS FOR AVOIDING VISHING

Vishing is quickly becoming one of the most common types of fraud. Protect yourself and your business with these simple tips.

1 BEWARE UNKNOWN NUMBERS

If you get an unknown call to your business mobile, then there's a chance this could be fraudulent. It is advised to let calls such as this go to voicemail, where a message can be left if it is someone with a genuine business matter.

2 DON'T ALWAYS TRUST CALLER ID

Criminals can cleverly manipulate technology to make it seem that they are representing a reputable business. Just because it appears that you are getting a call from your bank, for example, does not mean it is the case.

3 USE COMMON SENSE

Acknowledge when something appears out of place. Does your bank usually ring you at this time? Is someone offering something that seems too good to be true? Trust your instincts to recognise when something is not as it seems.

4 DON'T GET SWEPT UP IN URGENCY

Often, fraudsters will use tactics to get the information they need from you quickly, before you take a moment to think. It is very rare for a reputable business or institution to employ such behaviours, so this should be a warning.

5 ASK QUESTIONS

If you are contacted by someone who seems untrustworthy, ask them questions about their qualifications and credentials. If you don't receive clear or accurate responses, this should provide evidence that the caller is trying to commit fraud.

6 DON'T PROVIDE PERSONAL INFORMATION

Refrain from giving personal details, including things such as your name, job role and work address, until you can be sure the call is legitimate. Any details could potentially be used for future fraudulent activities.

7 BEWARE FALSE HANG-UPS

Fraudsters can play a disconnected sound, giving the impression that the call is over when it's not. If not finished properly, they may still be listening to subsequent conversations. Make sure the call is fully disconnected at its conclusion.

8 REPORT FRAUDULENT CALLS

Any calls that you believe could have been fraud should be reported, both internally and externally. If you believe there is a risk, you should report it to any external businesses that could be affected, such as your bank.

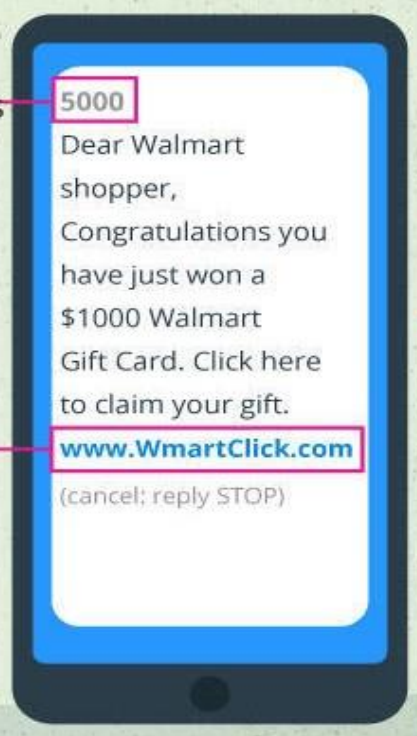
SMISHING

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

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

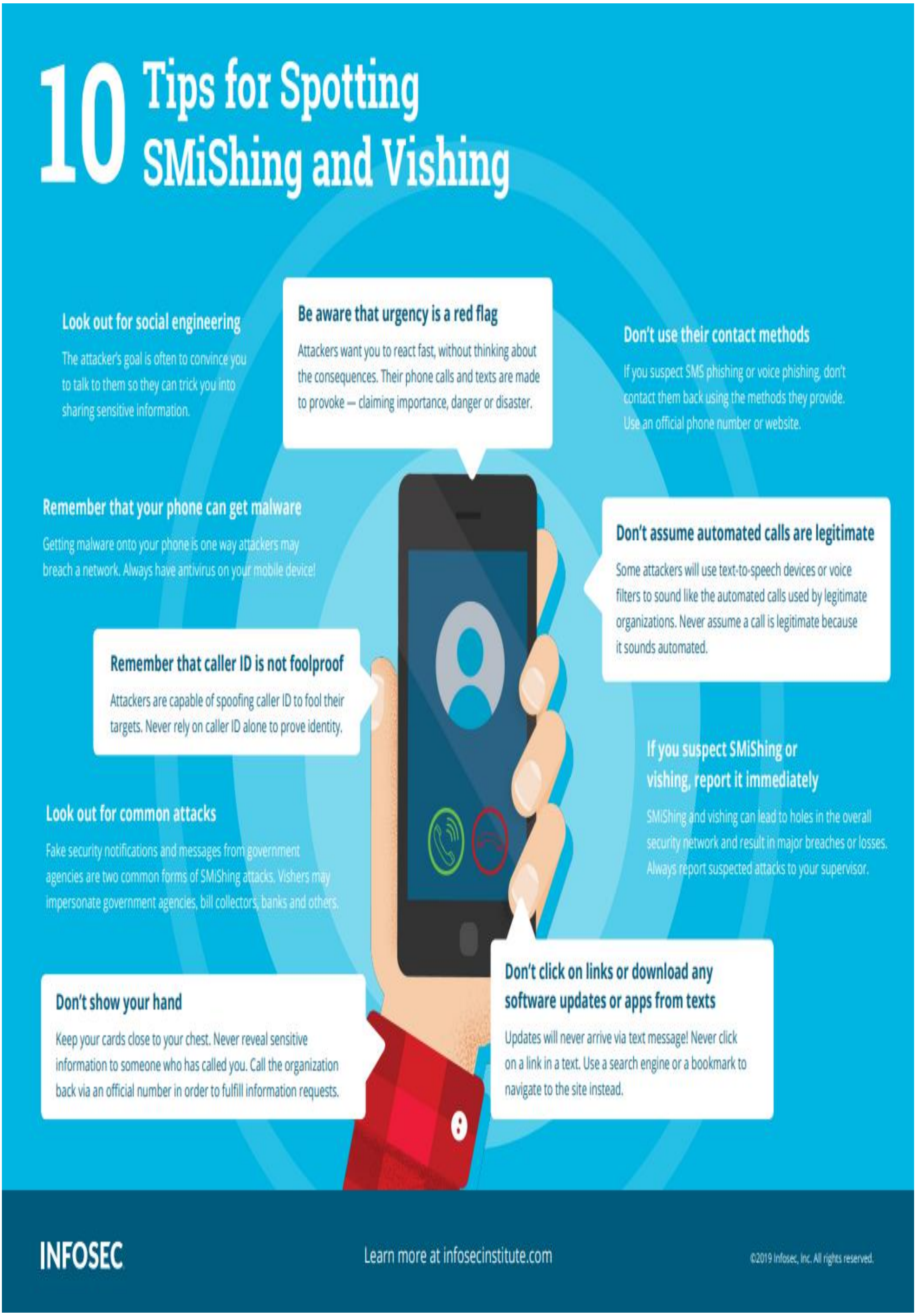
2 Attacker **poses as the victim** and asks Google for a **password reset**

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

4 **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."

5 Victim **sends the password verification code** to the smisher thinking that the request came from Google

6 Attacker uses the code to **reset the victim's password** and **take control** of their account


10 Tips for Spotting SMiShing and Vishing
Look out for social engineering
The attacker's goal is often to convince you to talk to them so they can trick you into sharing sensitive information.
Be aware that urgency is a red flag
Attackers want you to react fast, without thinking about the consequences. Their phone calls and texts are made to provoke — claiming importance, danger or disaster.
Don't use their contact methods
If you suspect SMS phishing or voice phishing, don't contact them back using the methods they provide. Use an official phone number or website.
Remember that your phone can get malware
Getting malware onto your phone is one way attackers may breach a network. Always have antivirus on your mobile device!
Don't assume automated calls are legitimate
Some attackers will use text-to-speech devices or voice filters to sound like the automated calls used by legitimate organizations. Never assume a call is legitimate because it sounds automated.
Remember that caller ID is not foolproof
Attackers are capable of spoofing caller ID to fool their targets. Never rely on caller ID alone to prove identity.
Look out for common attacks
Fake security notifications and messages from government agencies are two common forms of SMiShing attacks. Vishers may impersonate government agencies, bill collectors, banks and others.
If you suspect SMiShing or vishing, report it immediately
SMiShing and vishing can lead to holes in the overall security network and result in major breaches or losses. Always report suspected attacks to your supervisor.
Don't show your hand
Keep your cards close to your chest. Never reveal sensitive information to someone who has called you. Call the organization back via an official number in order to fulfill information requests.
Don't click on links or download any software updates or apps from texts
Updates will never arrive via text message! Never click on a link in a text. Use a search engine or a bookmark to navigate to the site instead.
INFOSEC
Learn more at infosecinstitute.com
©2019 Infosec, Inc. All rights reserved.