Smishing, Phishing and Vishing

Pig Butchering

Tech Support Scam

Scammers use social engineering tactics to create a sense of urgency, curiosity, or fear to manipulate the recipient into taking an undesired action.

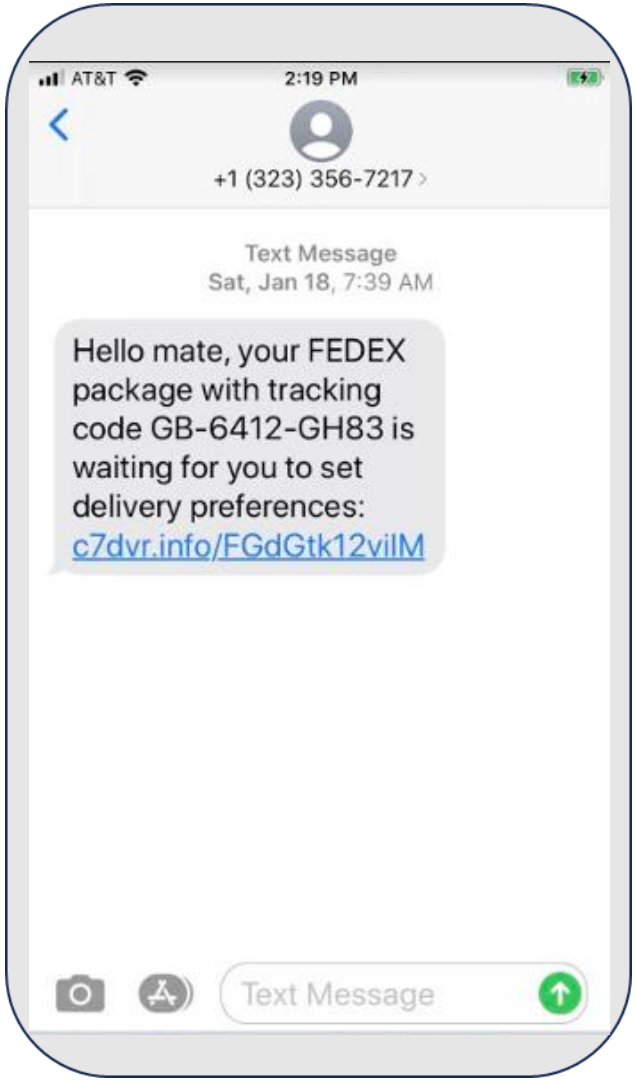
Smishing vs. Phishing vs. Vishing

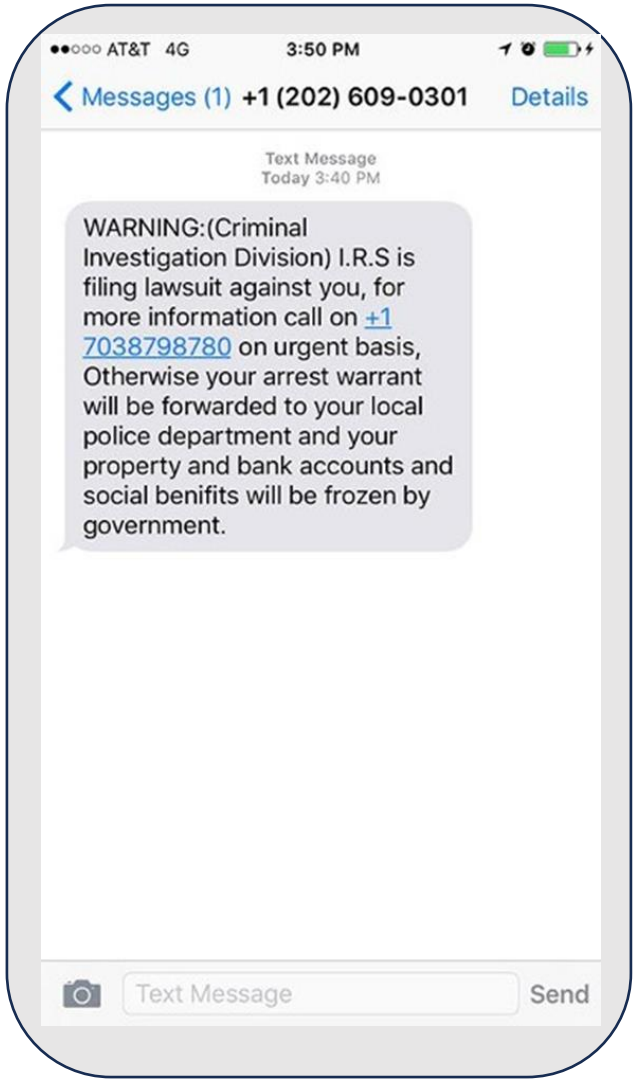
Smishing

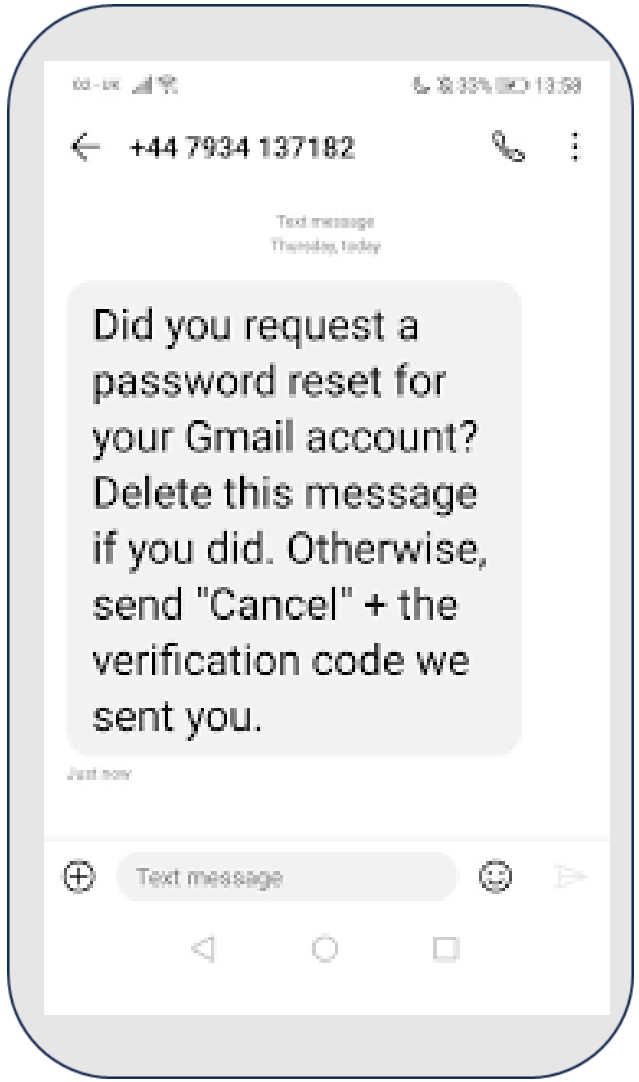
Smishing

- **Medium:** SMS (Short Message Service) or text messages.
- **Method:** Cybercriminals send deceptive text messages attempting to lure victims into sharing personal or financial information, clicking on malicious links, or downloading harmful software.
- **Example:** A text message alerting the recipient of a suspicious bank transaction and urging them to click a link to verify their account.

Smishing


AT&T
2:19 PM
+1 (323) 356-7217
Text Message
Sat, Jan 18, 7:39 AM
Hello mate, your FEDEX package with tracking code GB-6412-GH83 is waiting for you to set delivery preferences: c7dvr.info/FGdGtk12vilM
Text Message


AT&T 4G
3:50 PM
Messages (1) +1 (202) 609-0301
Details
Text Message
Today 3:40 PM
WARNING:(Criminal Investigation Division) I.R.S is filing lawsuit against you, for more information call on +1 7038798780 on urgent basis, Otherwise your arrest warrant will be forwarded to your local police department and your property and bank accounts and social benifits will be frozen by government.
Text Message
Send


+44 7934 137182
Did you request a password reset for your Gmail account? Delete this message if you did. Otherwise, send "Cancel" + the verification code we sent you.
Text message

Pig Butchering

What is ‘Pig Butchering’?
Pig butchering is a social engineering scam that combines elements of trust-building and fake investment opportunities. Here’s how it typically unfolds:

Initial Contact: The scam usually starts with a casual message sent via social media, dating apps, or even a random text message. Often, the scammer poses as a friendly acquaintance or romantic prospect. They may even open the conversation with an innocent-seeming “wrong number” text to lower the victim’s guard. For example, the scammer says, “Hi there! Is this John? This “mistaken” identity becomes a gateway for further engagement.

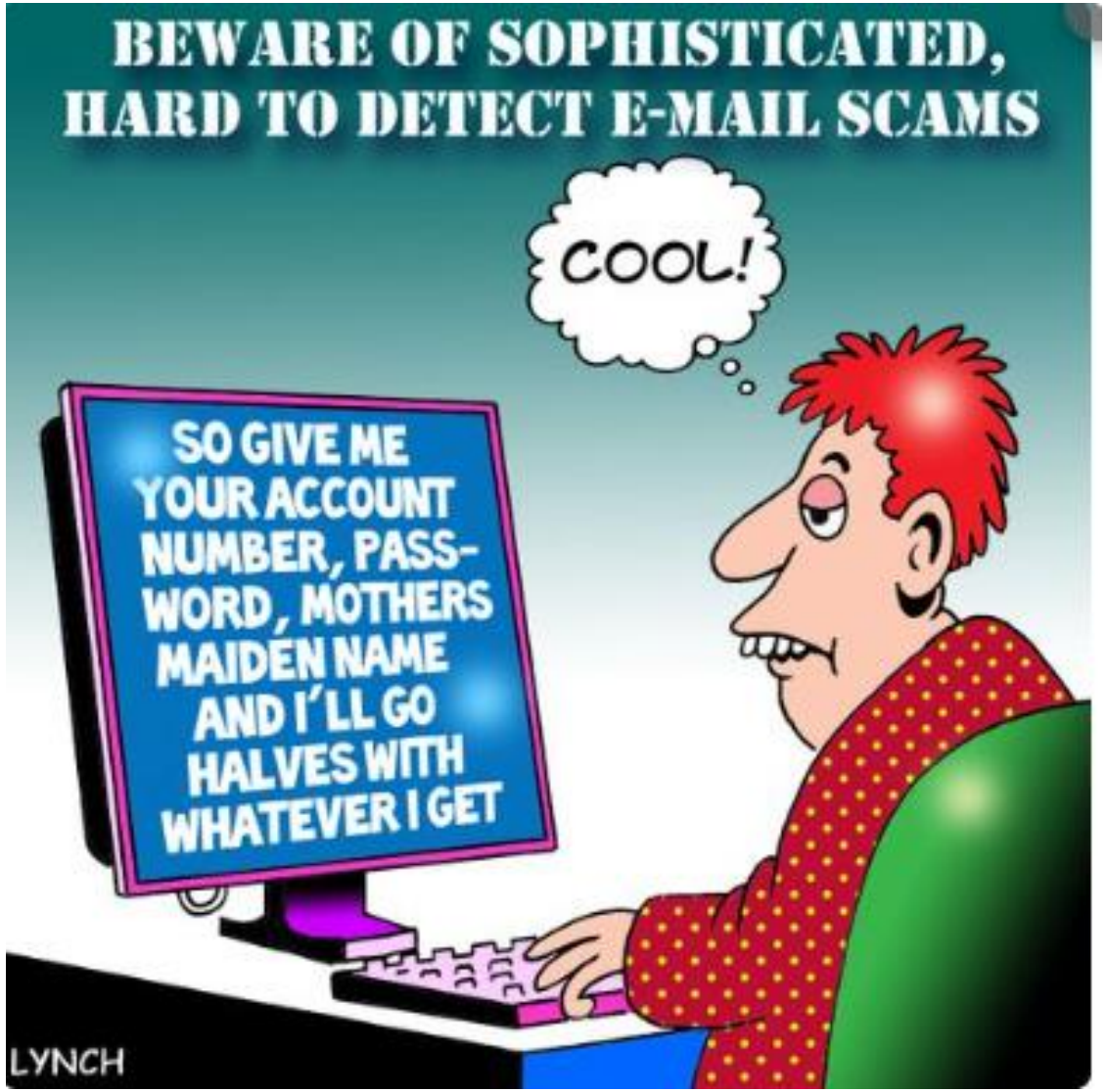
Building Trust: Over weeks or even months, the scammer works to gain the victim’s trust. They may send daily “good morning” messages, ask about the victim’s day, and gradually bring up their “successful” background in finance or investments. The scammer might say, “I’ve been working long hours at my finance job, but I really enjoy it. It’s given me financial freedom. Have you ever considered investing?”

Pig Butchering

Introducing the ‘Investment’: Once trust is built, the scammer starts mentioning a lucrative investment opportunity, often involving cryptocurrency or forex trading. They typically showcase “proof” of their own success with fake screenshots, making the scam appear legitimate. The scammer says, “Hey, I just made a 20% return on a crypto investment in two weeks. I’d be happy to show you how it works, no pressure.”

The Scam: The victim, feeling comfortable and encouraged, invests a small amount and may even see “returns” initially. Once the victim is confident and invests larger sums, the scammer disappears, taking the money with them.

Phishing

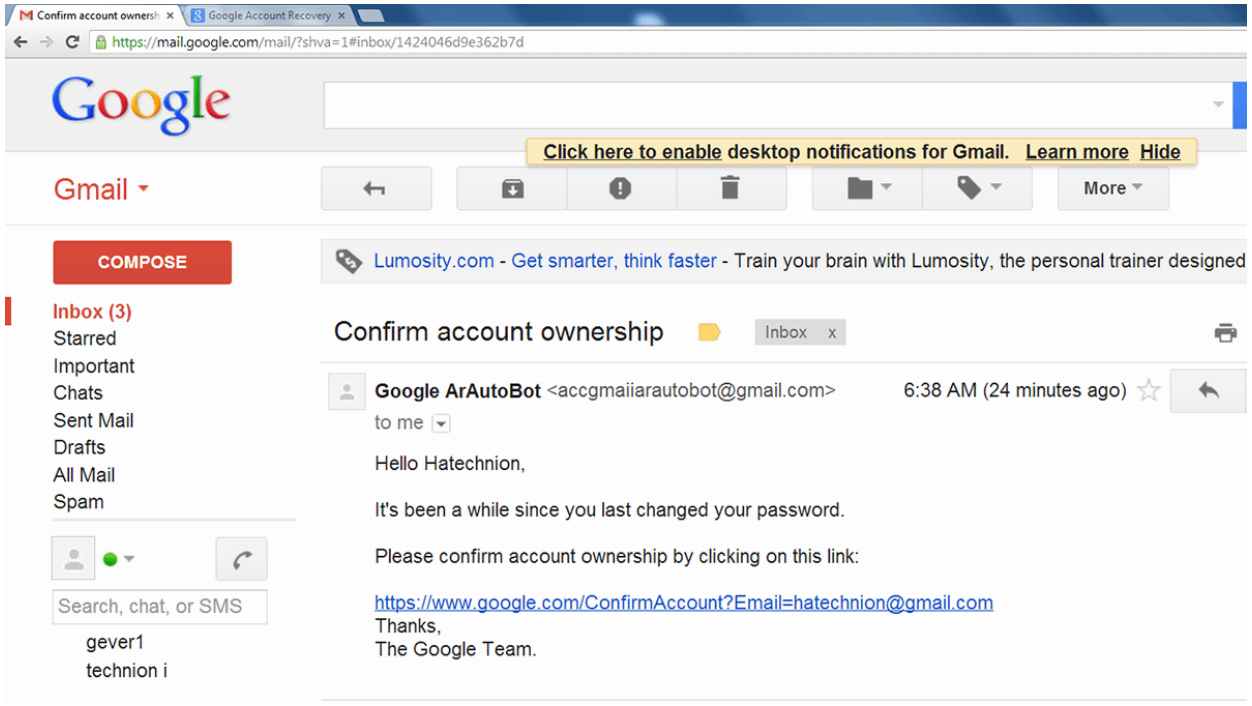

BEWARE OF SOPHISTICATED, HARD TO DETECT E-MAIL SCAMS
COOL!
SO GIVE ME YOUR ACCOUNT NUMBER, PASS-WORD, MOTHERS MAIDEN NAME AND I'LL GO HALVES WITH WHATEVER I GET
LYNCH

Phishing

Phishing

- **Medium:** Primarily email but can also include malicious websites and social media.
- **Method:** Cybercriminals craft fraudulent emails to appear as if they come from reputable sources. These emails often contain malicious links or attachments and are designed to trick recipients into providing sensitive data, such as login credentials or credit card numbers.
- **Example:** An email, seemingly from a popular e-commerce site, asking users to reset their passwords due to a security breach, leading to a fake login page.

Phishing



The attack is then carried out either when the victim clicks on a malicious file attachment or clicks on a hyperlink connecting them to a malicious website. In either case, the attacker's objective is to install malware on the user's device or direct them to a fake website. Fake websites are set up to trick victims into divulging personal and financial information, such as passwords, account IDs or credit card details.

Spear Phishing

REQUEST
Inbox

Grover Mudd <sutlejrd@virginmedia.com>
Nov 29, 2024, 2:18 PM
to me

Hi Mark,

I would like to know if you're available, Lydia needs to pay a vendor today but doesn't have Zelle or PayPal. Please let me know if you can help pay with either of this payment platforms. It's a program expenses for the association and it's urgent, Lydia will send you a reimbursement check if you can help. Please get back to me as soon as you get this.

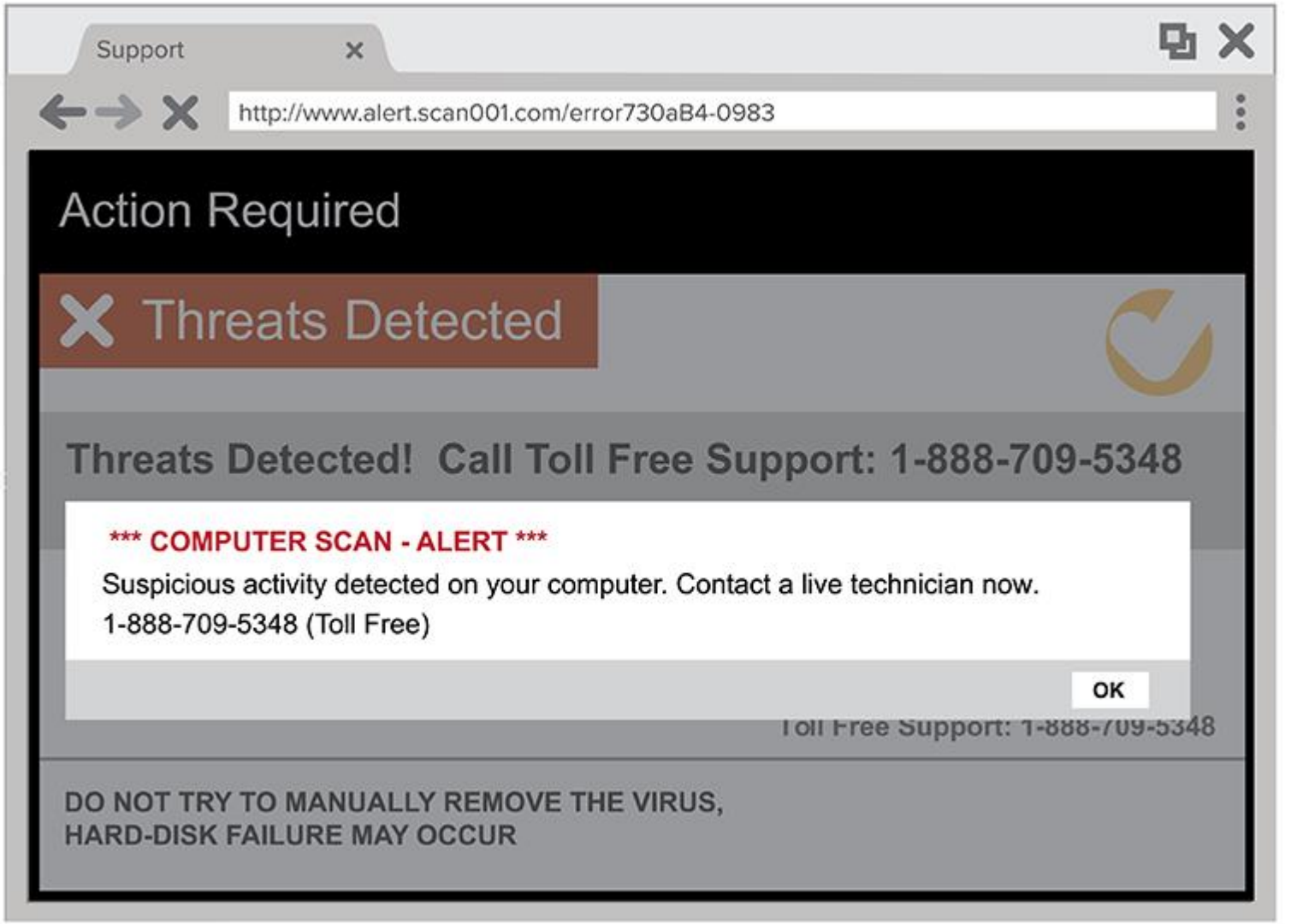
Regards
Grover Mudd

Vishing

Vishing (Voice Phishing)

- **Medium:** Voice calls (via traditional telephone or VoIP services).
- **Method:** Cybercriminals impersonate legitimate organizations, such as banks or government agencies, over the phone. They aim to extract sensitive information directly from the victim during the call.
- **Example:** A call from someone claiming to be from the IRS, stating that the victim owes back taxes and will face legal consequences unless they make an immediate payment.

Tech Support Scam



Tech Support Scam

Things To Know To Avoid a Tech Support Scam

1. Legitimate tech companies won't contact you by phone, email, or text message to tell you there's a problem with your computer.

2. Security pop-up warnings from real tech companies will never ask you to call a phone number or click on a link.

Key steps to take:

End the interaction: Hang up the phone or close the online chat window immediately.

Block contact details: Block the phone number and email address used by the scammer to prevent further contact.

Scan your computer: Run a thorough scan using reputable antivirus software to check for malware that the scammer might have installed.

Change passwords: Change the passwords for all your important accounts, including banking and email.

Contact your bank: Inform your bank about the potential scam and ask them to monitor your accounts for suspicious activity.

Report the scam: File a complaint with the Federal Trade Commission (FTC) online or by phone

Tips to avoid being scammed

Never Click Suspicious Links: If you receive an unexpected or suspicious text, refrain from clicking on any links or downloading attachments.

Verify Independently: If a text claims to be from a specific organization or individual, contact that entity directly using known contact information, not the details provided in the text.

Use Phone Security Features: Take advantage of built-in security features, like biometric authentication and regular software updates.

Don’t Share Personal Information: Never share personal, sensitive, or financial information via text unless you initiated the conversation and are certain about the recipient’s identity.

Check for Official Communication: Official organizations, especially banks and government agencies, typically don’t ask for personal information via text. If in doubt, call the organization directly.

Report a SCAM

FTC website at ReportFraud.ftc.gov

Call 1-877-FTC-HELP

"THIS IS A SPECIAL PLACE WE HAVE FOR PHISHING SCAMMERS!"


Any
Questions