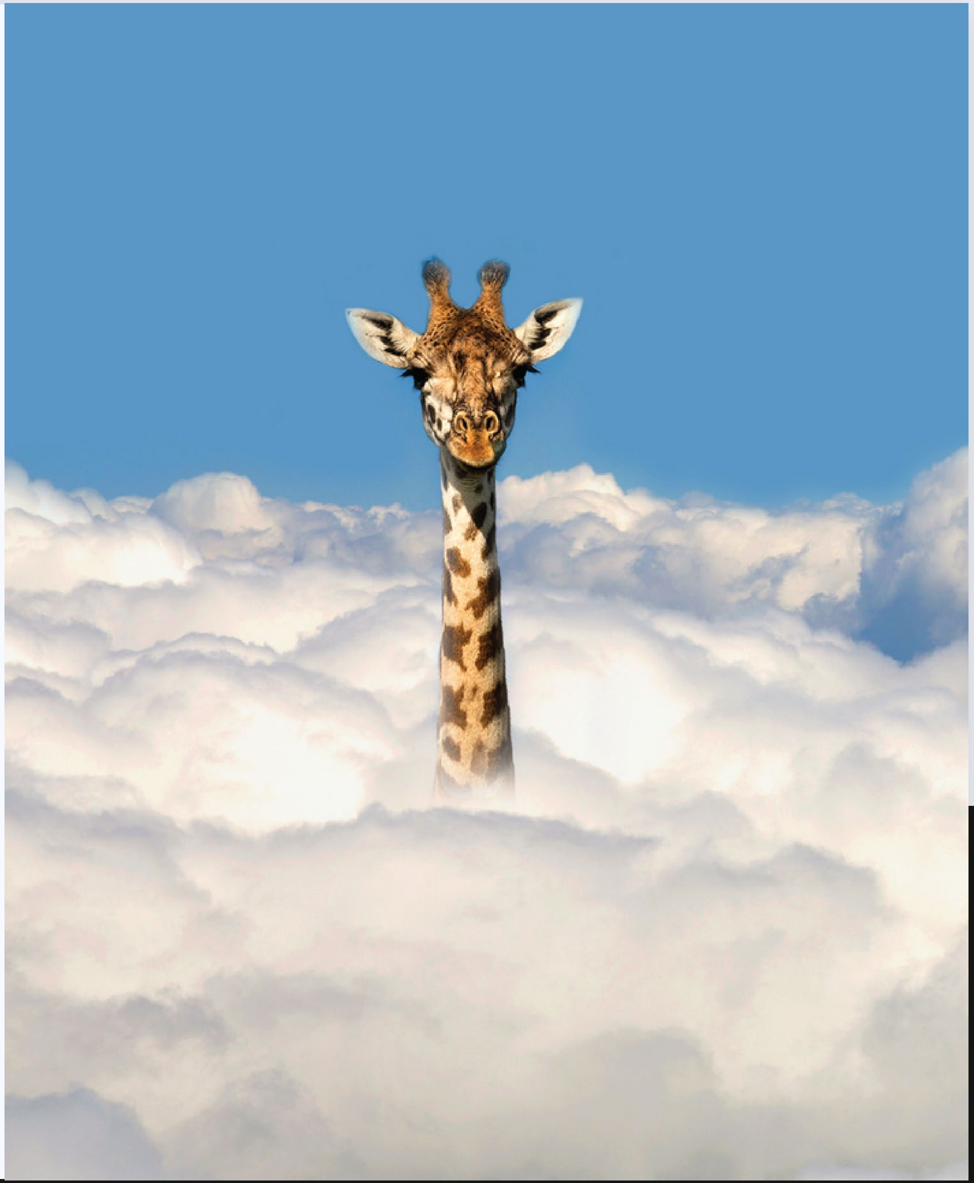
CYBERSECURITY AWARENESS

WHAT THREAT ACTORS LOOK FOR



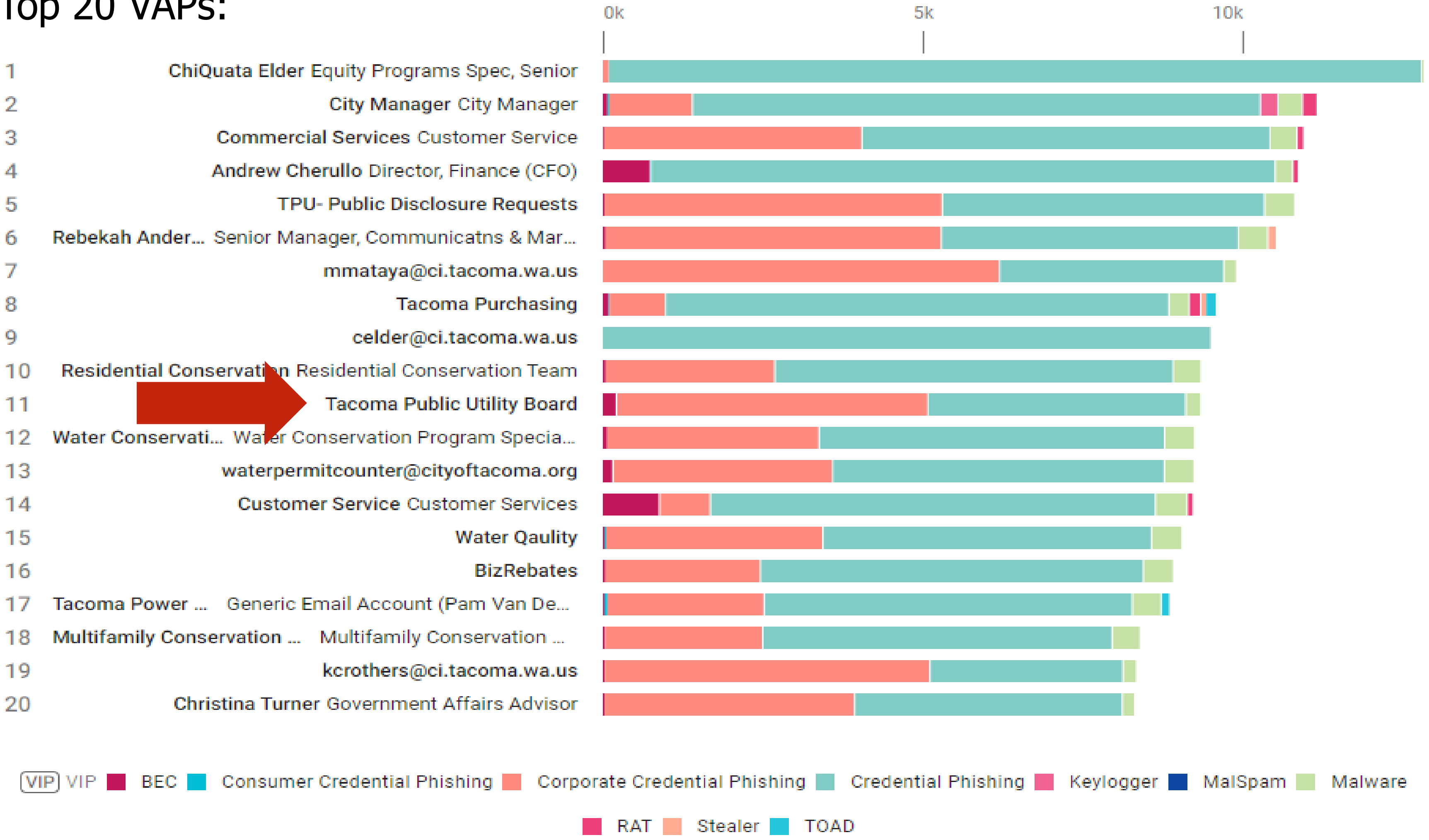
TOPICS

- PUBLIC UTILITIES BOARD ATTRACTIVENESS AND EXPOSURE TO CYBERSECURITY THREATS
- CURRENT RISK
- CONTROLS
- WHAT YOU NEED TO KNOW

City of Tacoma Data – Very Attacked People

140 e-mail addresses are attacked over 3.6x more often than the average workforce member.

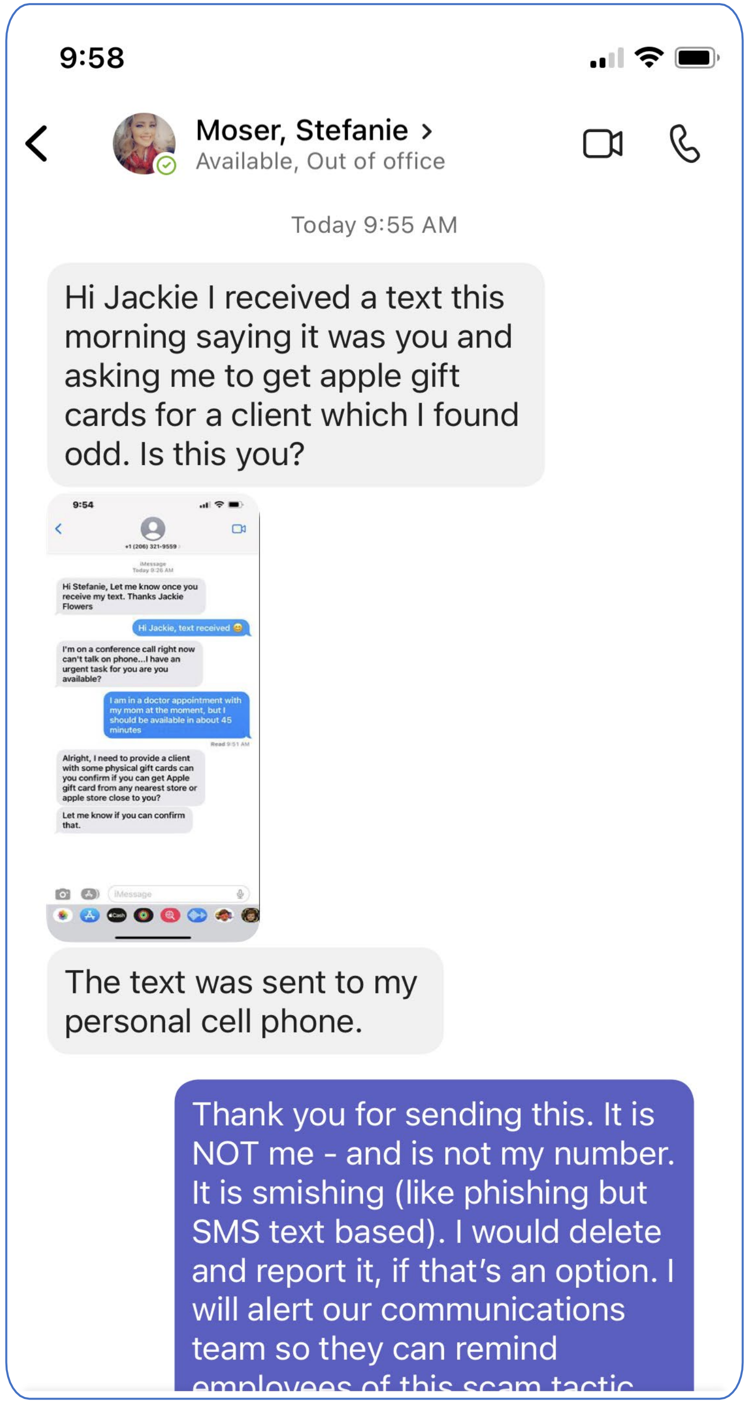
Top 20 VAPs:



Other prominent names:

Name	Rank
Tim Allen	33
Tory Green	34
Chris Robinson	69
Victoria Woodards	76
Adam Cook	80
Jackie Flowers	91
Shelby Fritz	97
Kristina Walker	102
Dale King	105
Scott Dewhirst	135
Catherine Ushka	133
Keith Blocker	138

Attack Failed Thanks to an Alert Employee



9:58

Moser, Stefanie
Available, Out of office

Today 9:55 AM

Hi Jackie I received a text this morning saying it was you and asking me to get apple gift cards for a client which I found odd. Is this you?

9:54

+1 (206) 321-9559

iMessage
Today 9:26 AM

Hi Stefanie, Let me know once you receive my text. Thanks Jackie Flowers

Hi Jackie, text received 😊

I'm on a conference call right now can't talk on phone...I have an urgent task for you are you available?

I am in a doctor appointment with my mom at the moment, but I should be available in about 45 minutes

Read 9:51 AM

Alright, I need to provide a client with some physical gift cards can you confirm if you can get Apple gift card from any nearest store or apple store close to you?

Let me know if you can confirm that.

iMessage

The text was sent to my personal cell phone.

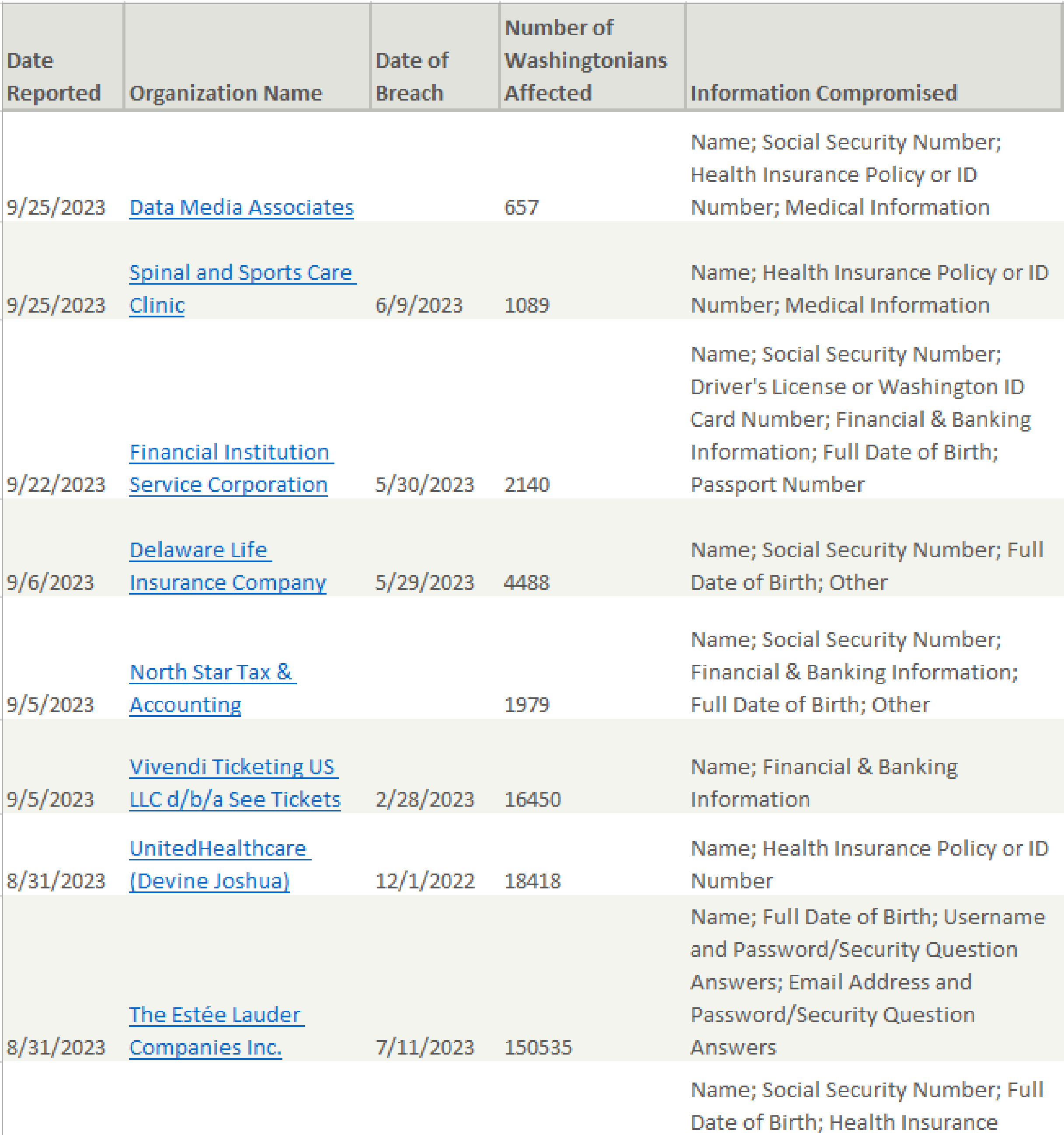
Thank you for sending this. It is NOT me - and is not my number. It is smishing (like phishing but SMS text based). I would delete and report it, if that's an option. I will alert our communications team so they can remind employees of this scam tactic

Prevalence of Attacks Locally

Washington State
Office of the Attorney General
Attorney General
Bob Ferguson

Visit Data Breach Notifications | Washington State to see breaches reported to the Attorney General.

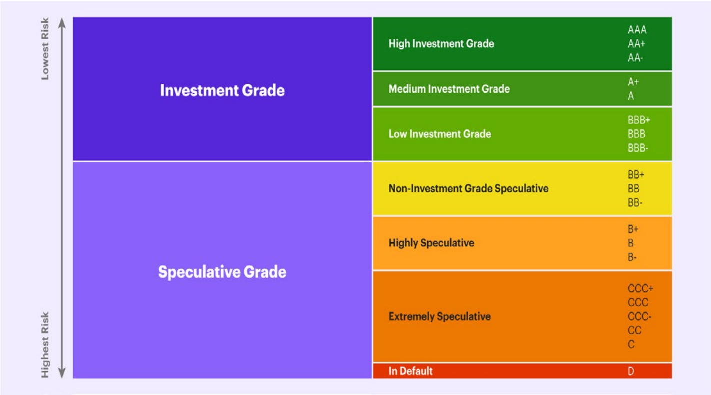
Company breaches in Washington from January 1 through September 2023 disrupted 124 companies and the lives of 2,915,713 Washingtonians who use their services.



Date Reported	Organization Name	Date of Breach	Number of Washingtonians Affected	Information Compromised
9/25/2023	Data Media Associates		657	Name; Social Security Number; Health Insurance Policy or ID Number; Medical Information
9/25/2023	Spinal and Sports Care Clinic	6/9/2023	1089	Name; Health Insurance Policy or ID Number; Medical Information
9/22/2023	Financial Institution Service Corporation	5/30/2023	2140	Name; Social Security Number; Driver's License or Washington ID Card Number; Financial & Banking Information; Full Date of Birth; Passport Number
9/6/2023	Delaware Life Insurance Company	5/29/2023	4488	Name; Social Security Number; Full Date of Birth; Other
9/5/2023	North Star Tax & Accounting		1979	Name; Social Security Number; Financial & Banking Information; Full Date of Birth; Other
9/5/2023	Vivendi Ticketing US LLC d/b/a See Tickets	2/28/2023	16450	Name; Financial & Banking Information
8/31/2023	UnitedHealthcare (Devine Joshua)	12/1/2022	18418	Name; Health Insurance Policy or ID Number
8/31/2023	The Estée Lauder Companies Inc.	7/11/2023	150535	Name; Full Date of Birth; Username and Password/Security Question Answers; Email Address and Password/Security Question Answers
				Name; Social Security Number; Full Date of Birth; Health Insurance

Regulators and 3rd parties consider security awareness training and periodic testing **minimum security controls.**

Absent controls affect:


Lowest Risk
Highest Risk

Investment Grade	High Investment Grade	AAA AA+ AA-
	Medium Investment Grade	A+ A
	Low Investment Grade	BBB+ BBB BBB-
Speculative Grade	Non-Investment Grade Speculative	BB+ BB BB-
	Highly Speculative	B+ B B-
	Extremely Speculative	CCC+ CCC CCC- CC C
	In Default	D

Bond Ratings and Interest Rates

Insurance Qualifications and Premiums

Contracts and Regulations

WHAT CAN WE DO TO IMPROVE RECOGNITION?

Social Engineering

When attempting to steal information or a person's identity, a malicious hacker will often try to trick you into giving out sensitive information rather than actually breaking into your computer.

Example

Targeted Attack

To ensure success, social engineers will first do reconnaissance, learning as much as they can about their target before placing a call or showing up at an office. For example, through Facebook and online searches, an attacker learns where the target lives, that she participates in fundraisers for cancer research, and the name of her favorite restaurant.

The social engineer then calls, posing as a fundraiser and offering a free dinner at the target's favorite restaurant, in exchange for a modest donation. When she agrees, the social engineer sends her a "coupon." Of course, it's actually an infected PDF file, which once opened, installs spyware on her computer.

Best
Practices

To prevent social engineering attacks from succeeding, follow these best practices:

- Always be suspicious when someone asks for sensitive information, especially your username and password,
- Verify the identity of those who ask for information in person or over the phone before you release it,
- Do not give out information about other employees, remote network access, organizational practices, or strategies to any unknown individual, and
- Limit the amount of personal information you publicly share on the web, especially on social networking sites.

Online Threats and Vulnerabilities

Offline threats tend to be more obvious than online threats, which can be very subtle and intentionally hidden.

Phishing

Phishing is a type of social engineering that happens online via email. A typical scam is sending out a spam email that looks like it is coming from a legitimate bank. The email might, for example, ask you to "verify" your account number and PIN and redirect you to a website that looks just like the bank website, but when you enter your information, it goes directly to the phisher.

Phishing

Click on each icon below to learn about best practices for avoiding phishing scams.

Urgent!!! +

Links and URLs +

HTTPS +

Urgent!!!

Never respond to unsolicited email messages that request personal information and use sensational phrases like "URGENT!!!". A reputable company will never ask you for your password.

CLOSE

Links and URLs

Always navigate to your bank or other financial institution's website by typing in the official website address into your browser rather than clicking a link from an unsolicited spam email message.

And never click on or open attachments sent with spam email messages.

CLOSE

HTTPS

Make sure that any website that you visit that contains or requests personal information is secure. Look for “HTTPS” in the web address or a padlock icon in your browser window.

If a site is not secure, do not give out any personal information. Be aware however, that even malicious sites may be secure.

CLOSE

Spear Phishing

Phishers can steal more money by targeting a select group, or a few individuals, with a highly tailored message. This is known as spear phishing and is much harder to counter because the messages can seem so authentic.

For example, an attacker could conduct an online search, quickly compiling a list of names, email addresses, and job titles. The attacker can then send out an email message that appears to be coming from a colleague, discussing a relevant topic. This makes it much harder to resist opening an infected attachment or clicking on an infected link.

Thwart Spear Phishing
Attacks

Pet Lover

@CorinePetLover

My chocolate brown golden doodle Buster - just won best in show!

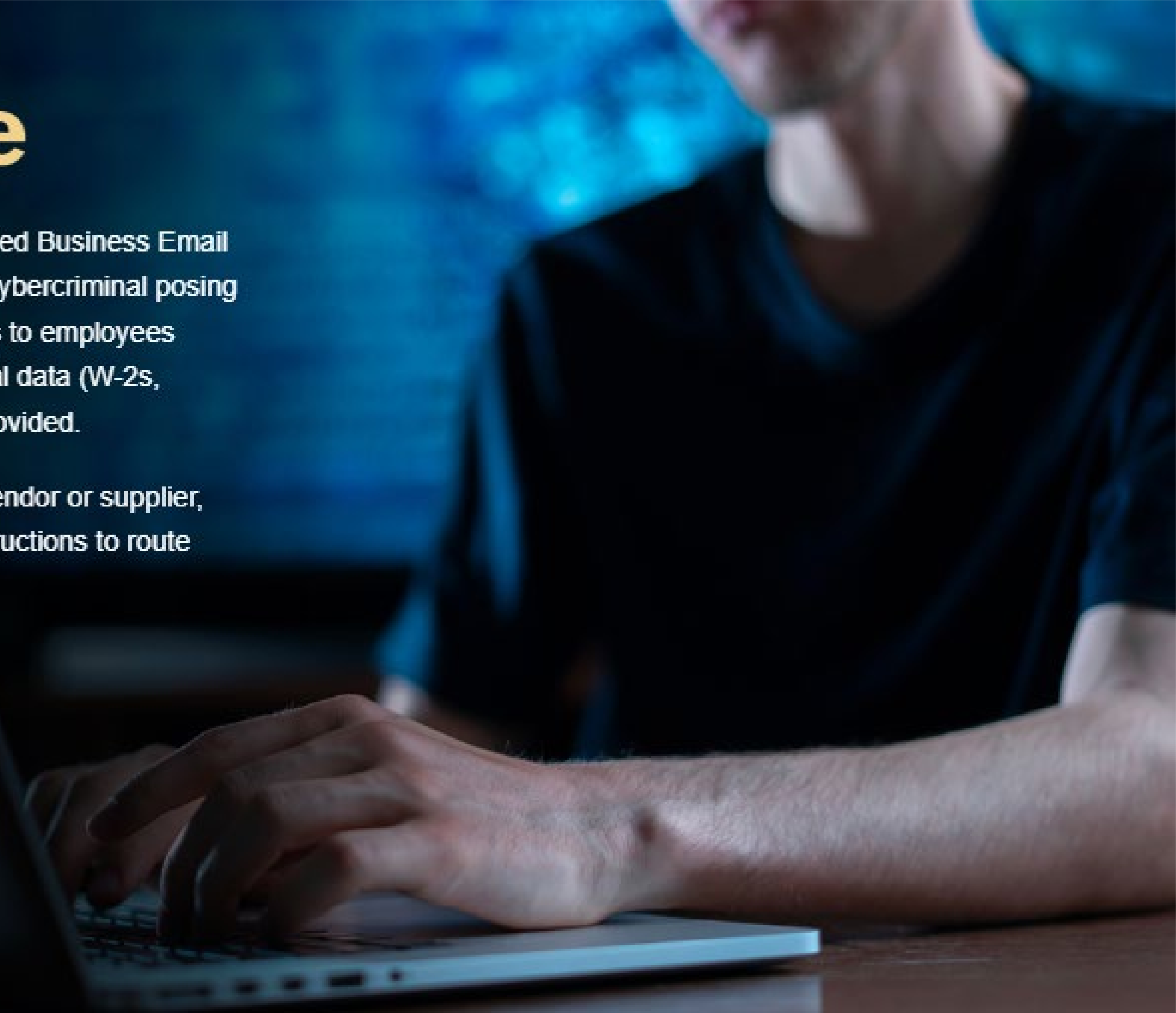
To thwart spear phishing attacks:

- If a suspicious-looking email arrives from someone you trust, call them or email them separately and ask if they sent it before opening the email, clicking on any links, or opening any attachments, and
- Keep in mind that anything you've posted on social networks can be used in spear phishing emails to make them seem legitimate.

(BEC) Business Email
Compromise

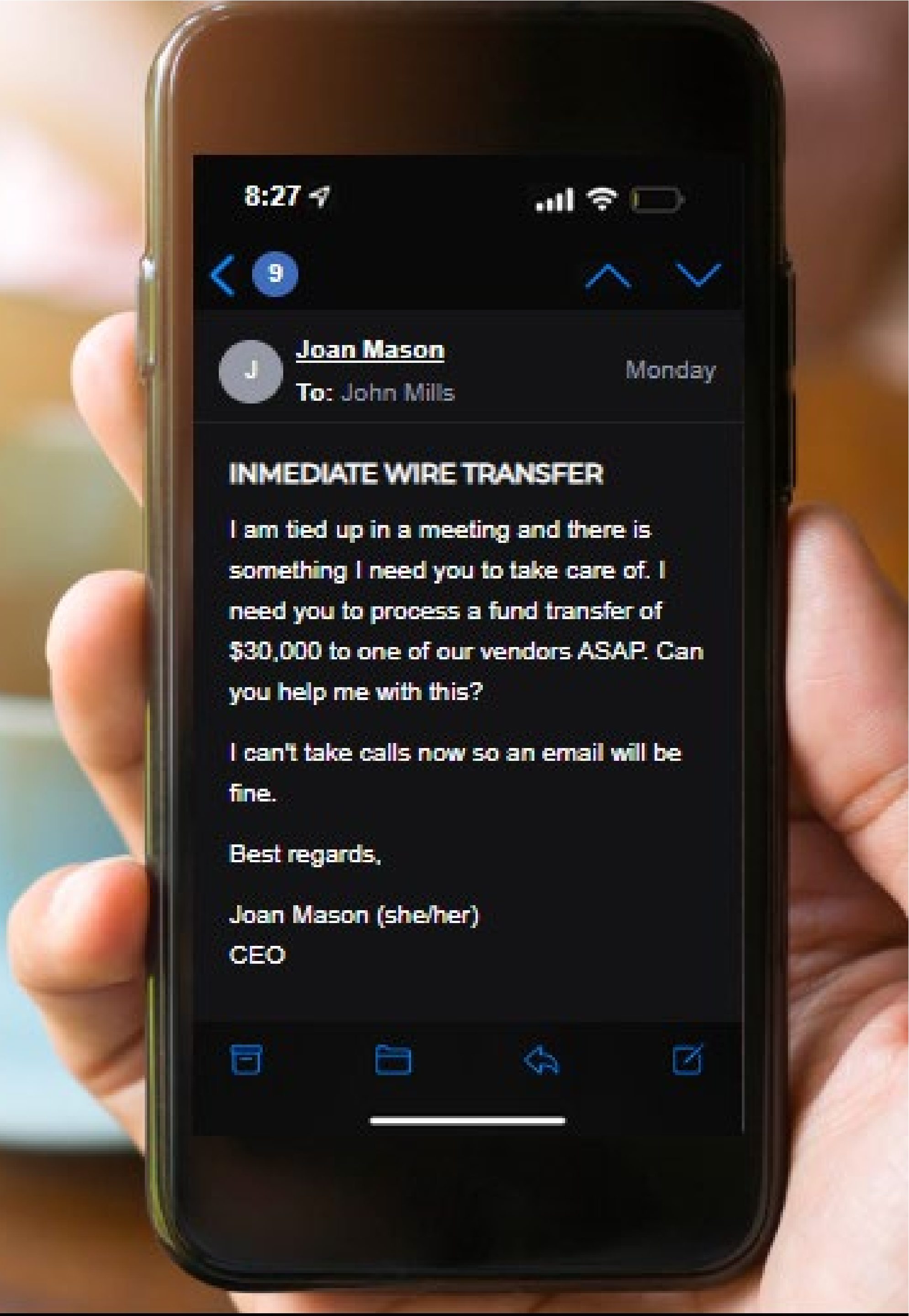
A scam that has been on the rise recently is called Business Email Compromise or BEC. Typically, this involves a cybercriminal posing as an executive or manager and sending emails to employees requesting funds to be transferred or confidential data (W-2s, Personally Identifiable Information (PII), etc.) provided.

Additionally, cybercrimals may impersonate a vendor or supplier, and send fake invoices or change payment instructions to route money into their accounts.



(BEC) Business Email
Compromise

Many times, these communications are sent through "spoofed" email addresses that resemble the actual email address of the person they are posing as. They may even hijack the actual email account of the person, making it much more difficult to tell if it's a legitimate request or a potential scam.



Joan Mason
To: John Mills
Monday

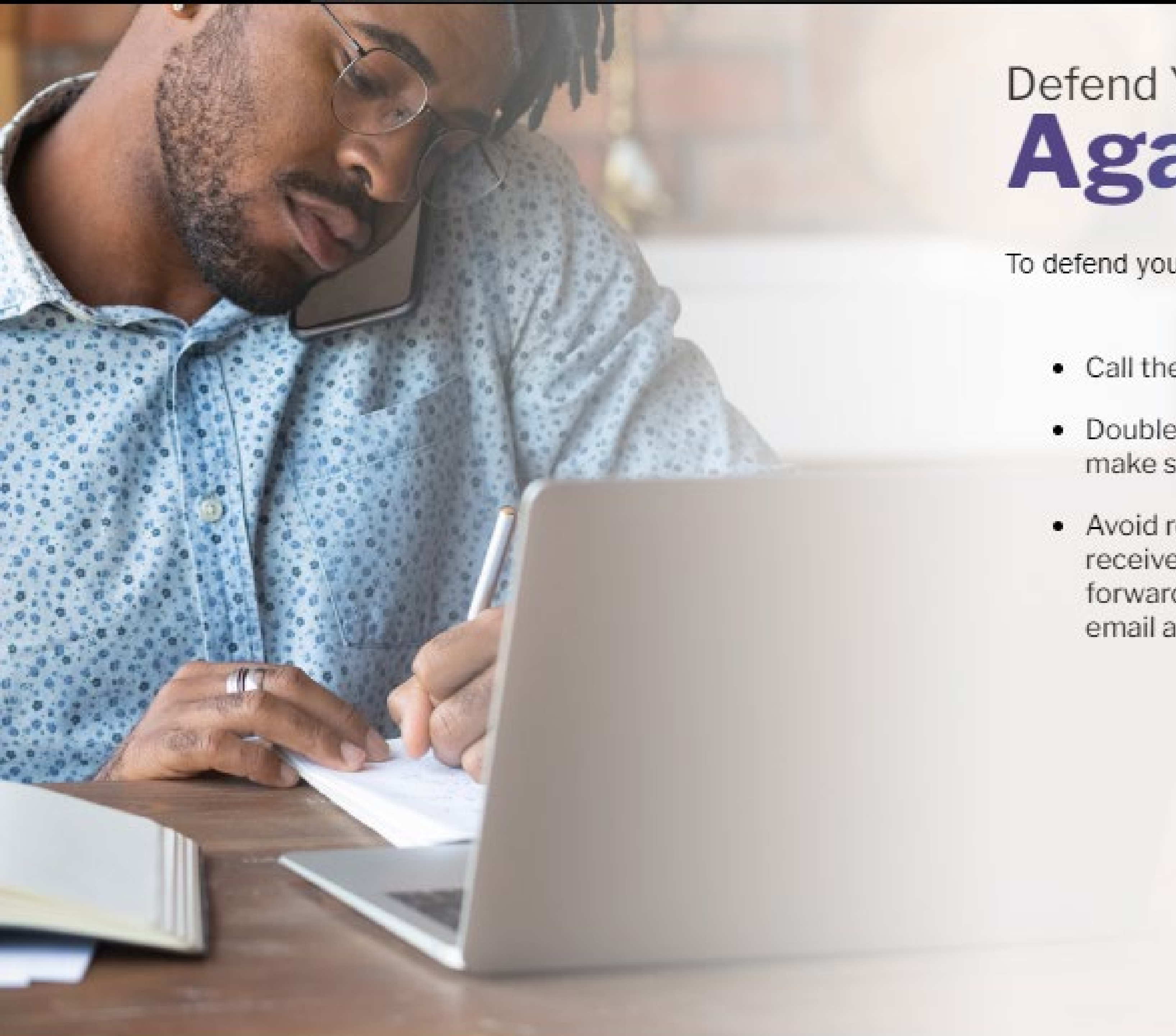
INMEDIATE WIRE TRANSFER

I am tied up in a meeting and there is something I need you to take care of. I need you to process a fund transfer of $30,000 to one of our vendors ASAP. Can you help me with this?

I can't take calls now so an email will be fine.

Best regards,

Joan Mason (she/her)
CEO



Defend Yourself Against BEC

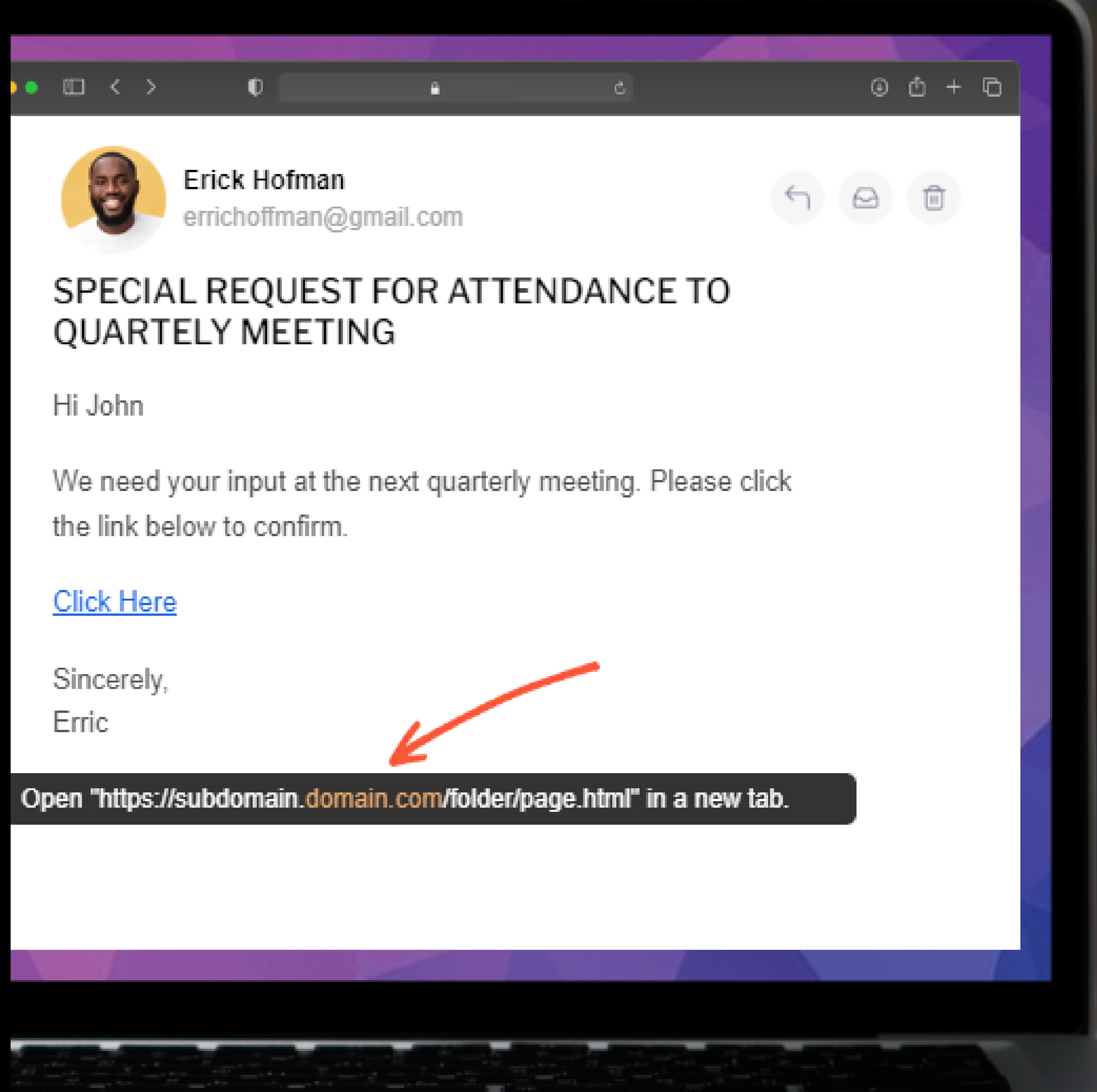
To defend yourself against BECs, follow these best practices:

- Call the sender to verify that the request is legitimate,
- Double-check the email address of the sender to make sure it isn’t being spoofed, and
- Avoid replying to the sender, especially if this is being received from a personal email address. Instead, forward your response to the sender’s actual work email address.

Defend Yourself Against BEC

- Be wary of changes in how the sender communicates, especially if you are asked to maintain secrecy or if the tone is urgent, and
- If you receive a request to change payment instructions, this should be an immediate red flag. Always call the sender with a phone number you have on file and not located within the email itself.

If you do fall victim to a BEC, it is **very important** to alert your manager quickly. If funds were transferred, there is a chance to freeze the process and recover the funds.



Erick Hofman
errichoffman@gmail.com

SPECIAL REQUEST FOR ATTENDANCE TO QUARTELY MEETING

Hi John

We need your input at the next quarterly meeting. Please click the link below to confirm.

Click Here

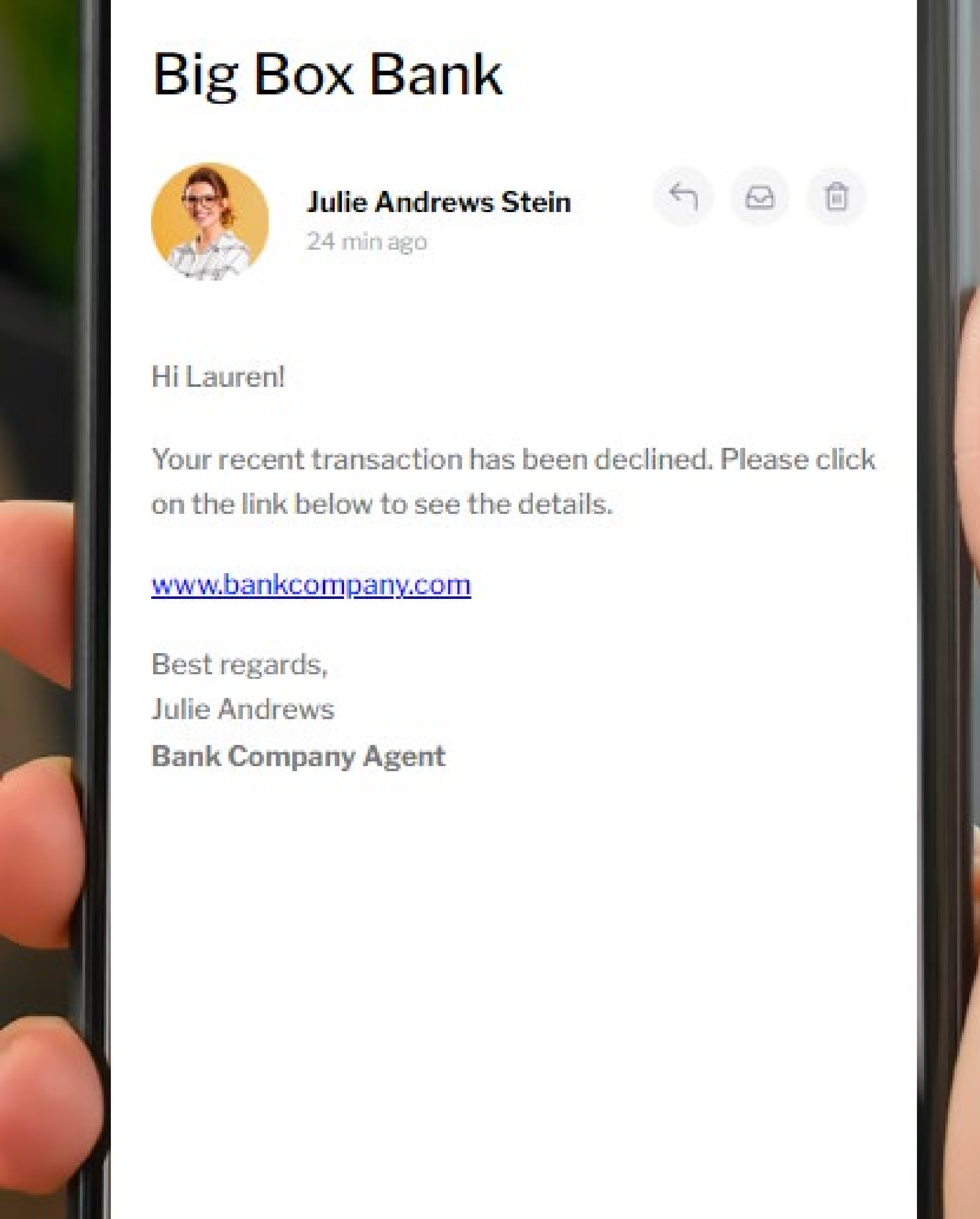
Sincerely,
Erric

Open "https://subdomain.domain.com/folder/page.html" in a new tab.

Identifying Malicious URLs

Another way to defend yourself from phishing attacks is to recognize a fake website by looking at the URL (Uniform Resource Locator). The key thing to remember is that the end of the URL, before the first single forward slash ("/"), is what matters. You should ignore the subdomain, folder, and page name.

Hover over links in email, SMS and instant messages, and on websites to verify the actual URL, even if the link comes from a trusted source.



Big Box Bank

Julie Andrews Stein
24 min ago

Hi Lauren!

Your recent transaction has been declined. Please click on the link below to see the details.

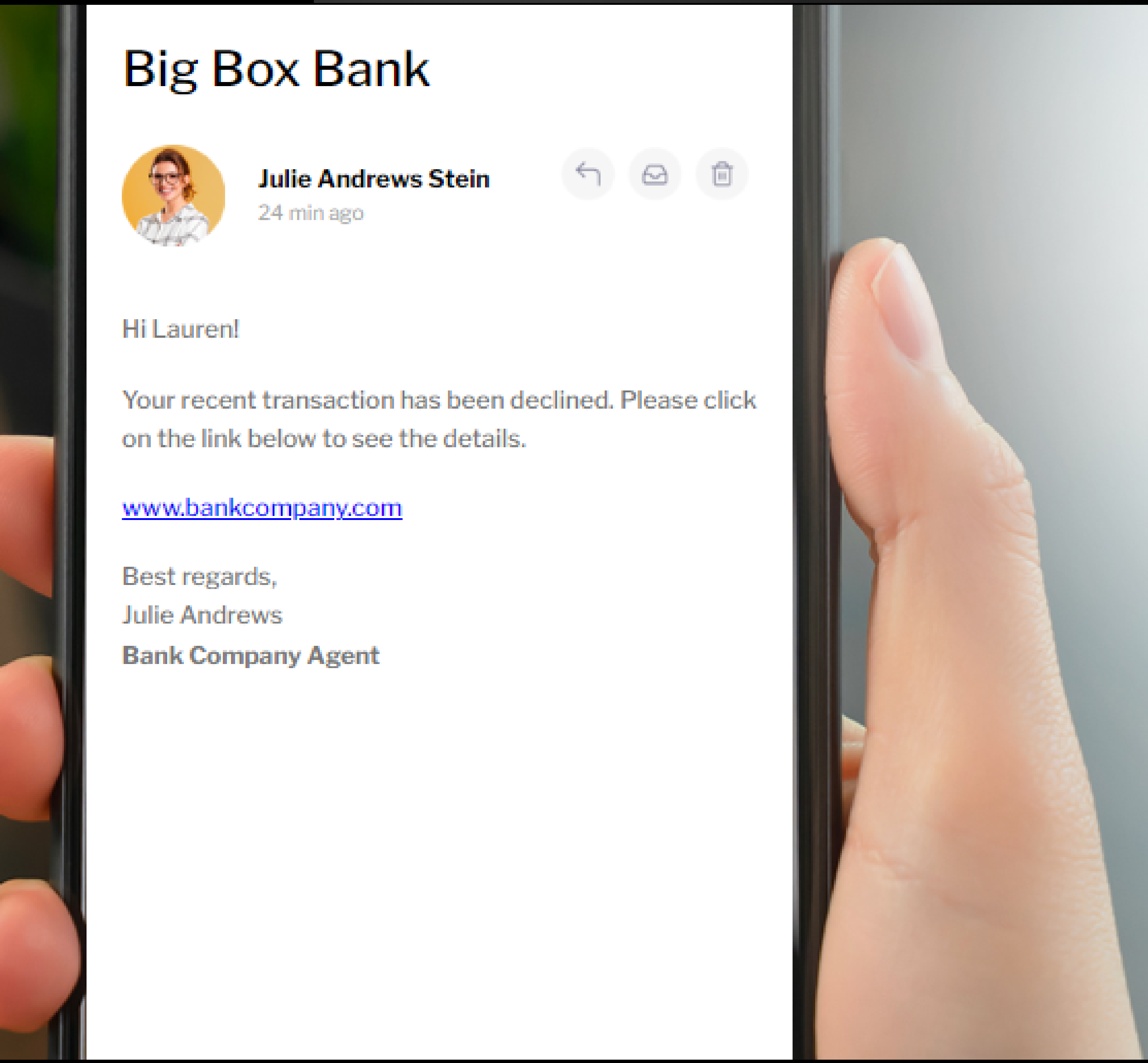
www.bankcompany.com

Best regards,
Julie Andrews
Bank Company Agent

Mobile: Identifying URLs

To identify URLs on most mobile devices, simply hold your finger down on the link (long press) which will pop up and reveal the intended address.

Be aware however that a URL can be masked in an email by using a button instead of a link. If you don't see a URL address, it's best to navigate instead to the homepage of your bank or other websites by typing in the website address in your browser.



Big Box Bank

Julie Andrews Stein
24 min ago

Hi Lauren!

Your recent transaction has been declined. Please click on the link below to see the details.

www.bankcompany.com

Best regards,
Julie Andrews
Bank Company Agent

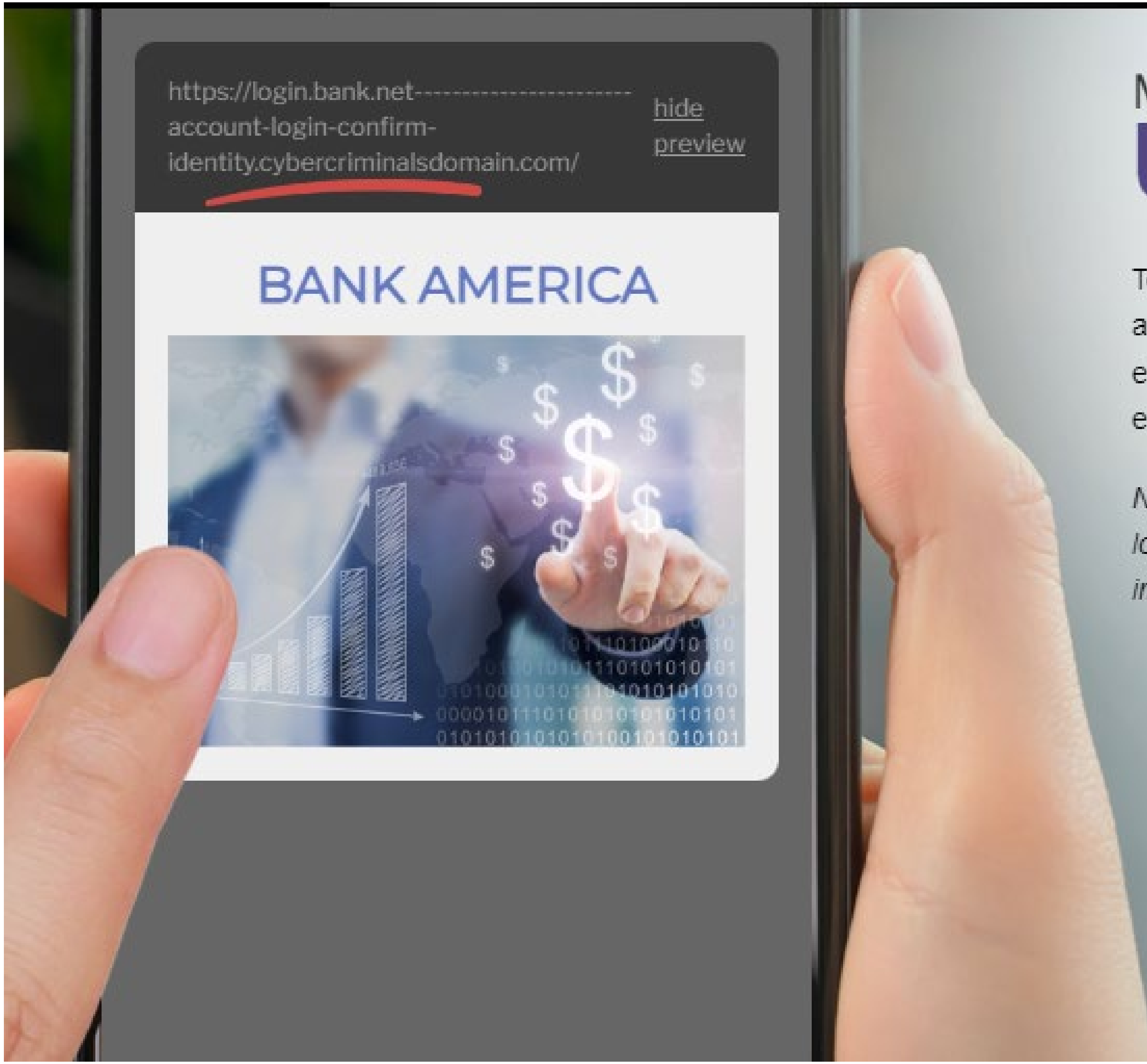
Mobile: URL Padding

Cybercriminals do have a way to make identifying malicious URLs more difficult on mobile devices.

For example, when viewing the destination of a link in a smartphone, there is limited space for showing the full URL. Thus cybercriminals will lengthen or "pad" the URL with hyphens or other characters to push the actual destination outside of the viewing area, while still tricking you into seeing what looks like a legitimate destination at first glance.

m.facebook.com----------
validate.rickytaylk.com/sign_in.html

accounts.craigslist.org-secureloging--------------------
viewmessage.model104.tv/craig2/icloud.com--------
secureaccount-confirm.saldaodovidro.com.br


https://login.bank.net------------------------account-login-confirm-identity.cybercriminalsdomain.com/
hide preview
BANK AMERICA

Mobile:

URL Padding

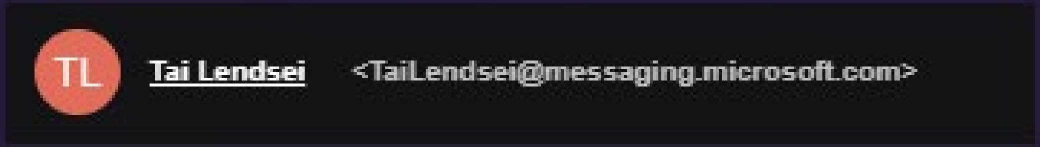
To avoid this trick, pay close attention to the website address for signs of padding. You can also view the email or website over a computer where you can more easily view the complete address.

Note: You can practice identifying a URL by hovering (or long-tapping) the hyperlink icon on the smartphone image to the left.

Mobile: Spoofing is

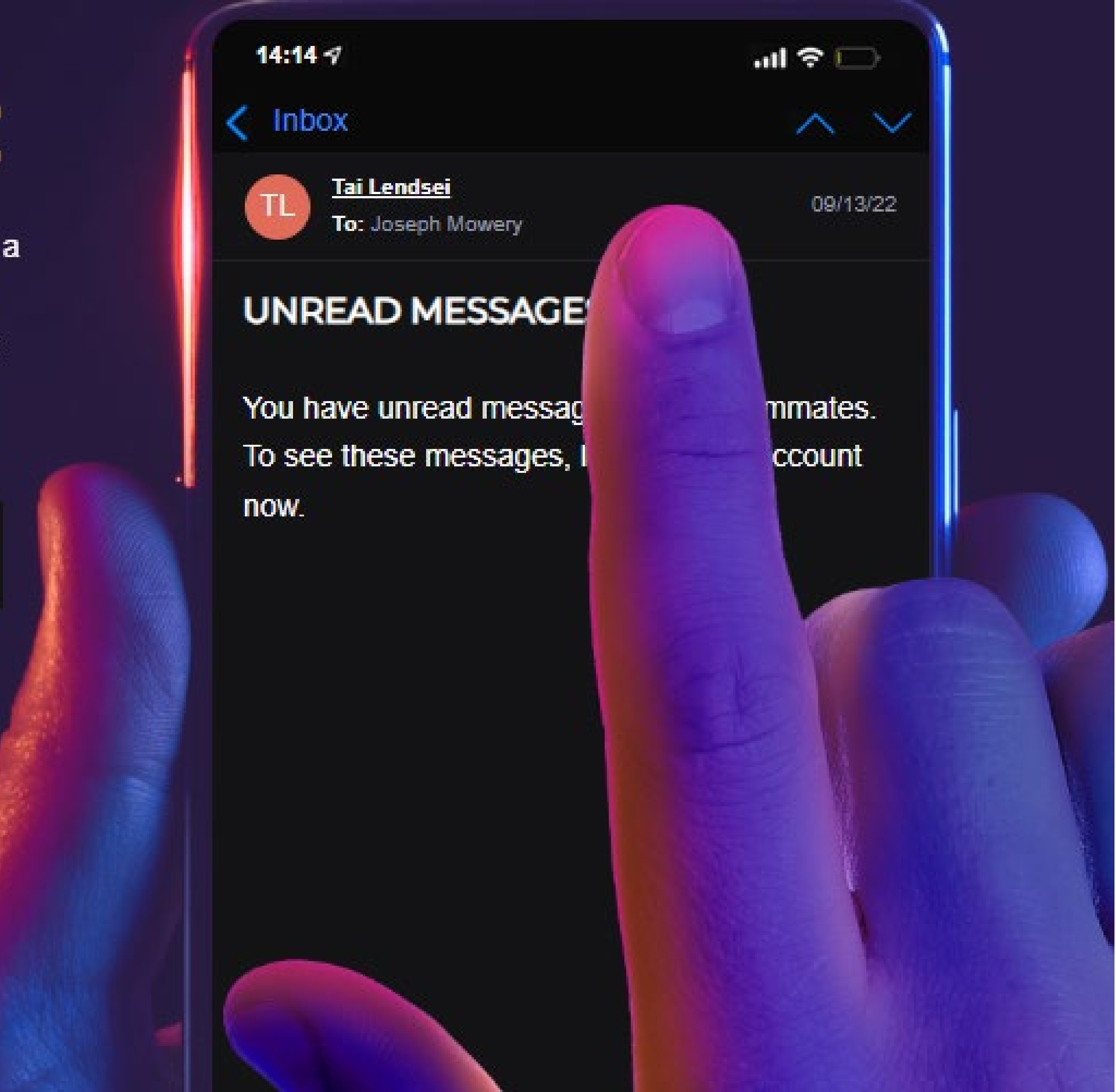
Harder to Spot

It's very easy to spoof a legitimate email address to show a different sender's name which appears legitimate. When viewing an email address on a desktop or laptop, you can see the real email address off to the side surrounded by angle brackets (<>).



TL **Tai Lendsei** <TaiLendsei@messaging.microsoft.com>

However, on a smartphone, this can be trickier to spot. These email addresses are not displayed at first, only the sender's name. You have to click the sender's name to reveal the true email address.



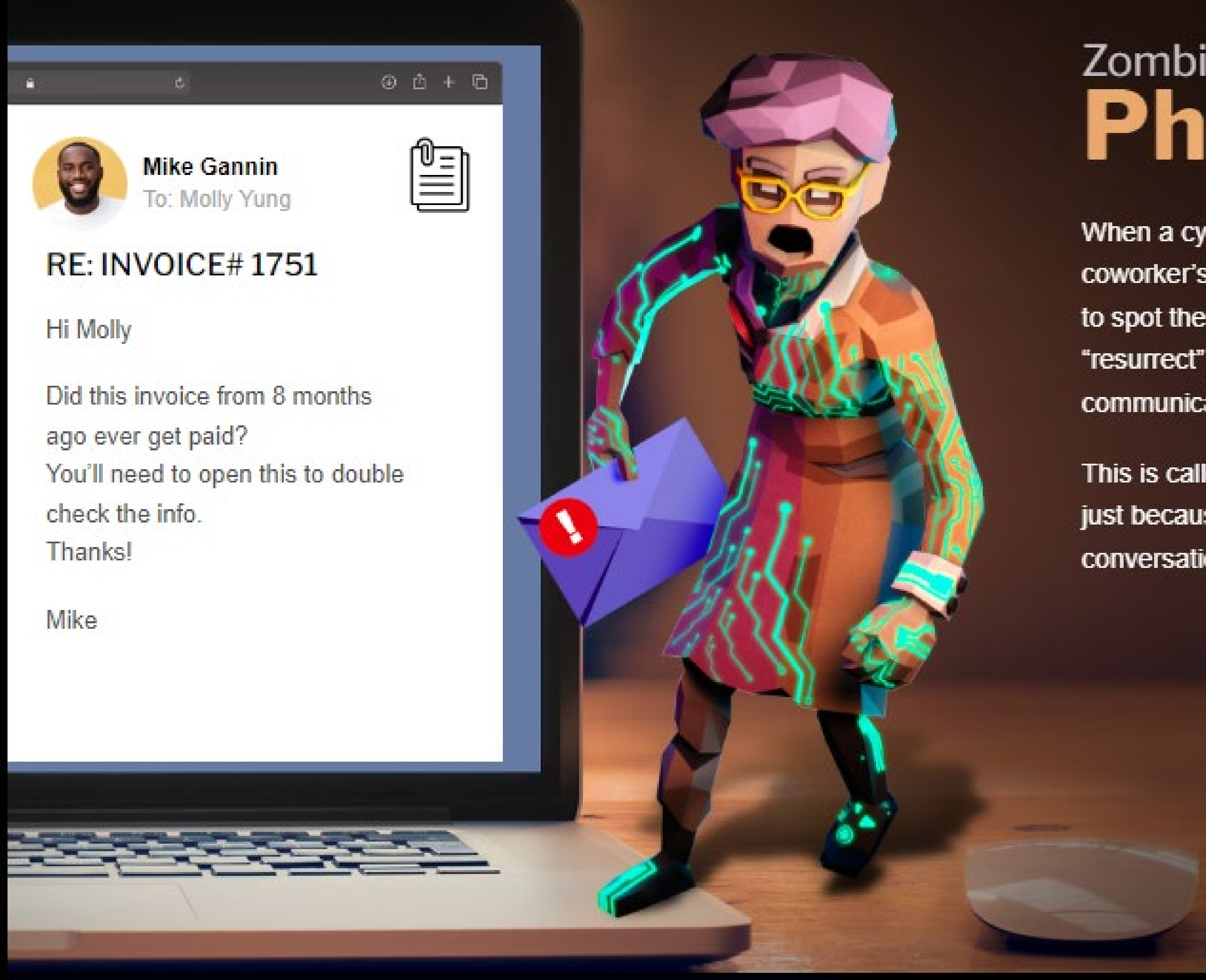
Tai Lendsei

To: Joseph Mowery

09/13/22

UNREAD MESSAGE

You have unread messag mmates. To see these messages, l ccount now.



Mike Gannin
To: Molly Yung

RE: INVOICE# 1751

Hi Molly

Did this invoice from 8 months ago ever get paid?
You'll need to open this to double check the info.
Thanks!

Mike

Zombie Phish

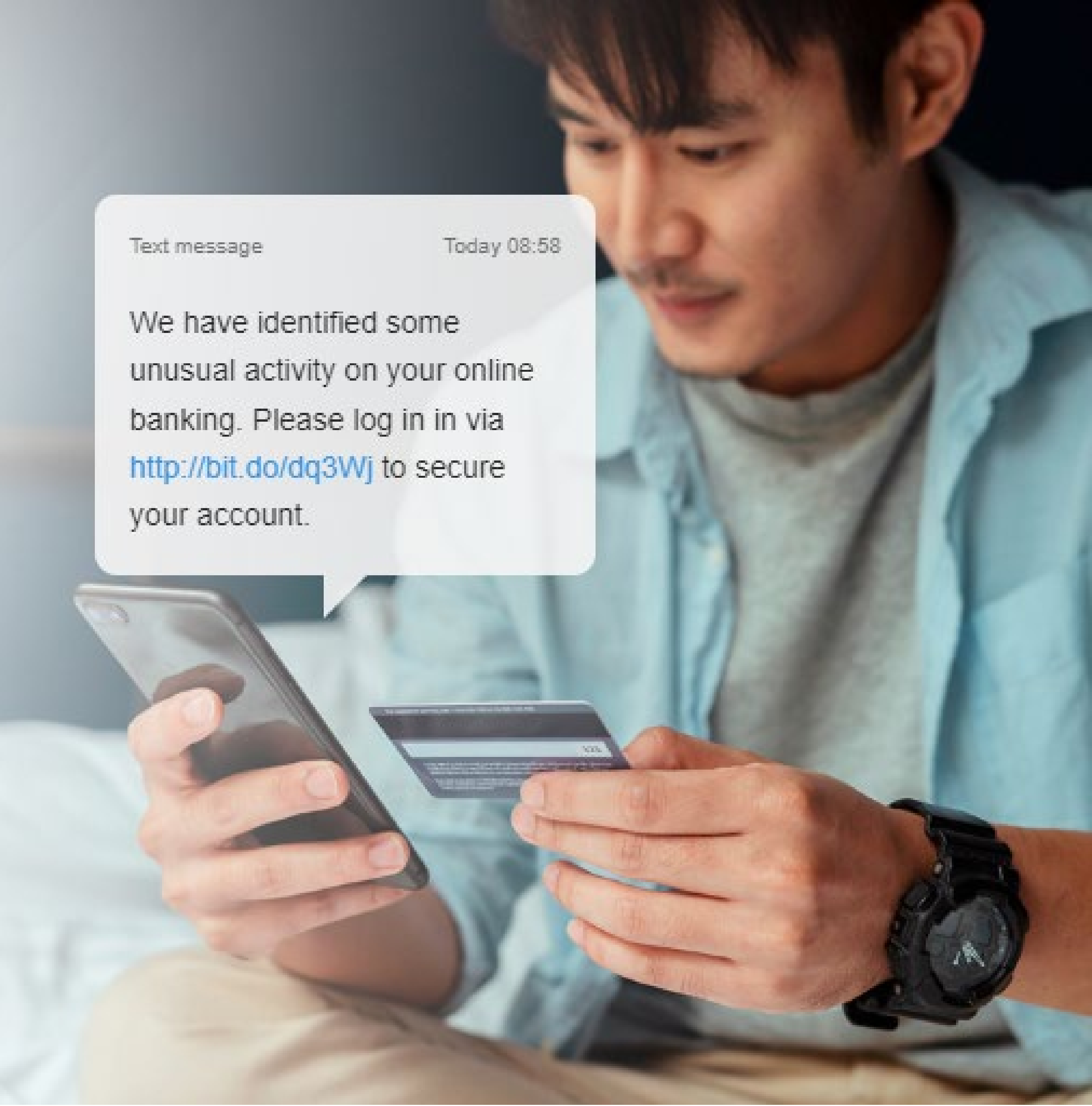
When a cybercriminal has compromised a coworker's email account, it can be especially tricky to spot the phishing attempt. Phishers will sometimes "resurrect" an older email thread to make the communication seem even more genuine.

This is called a "Zombie Phish." So, don't be fooled just because a suspicious email is tied to a previous conversation.

Other Phishing
Attack Vectors

Also, keep in mind that email is not the only source of phishing messages. Online criminals also target SMS text messages (SMiShing), social networking sites, and even voicemail.

And instead of directing you to a spoofed website, you may be directed to call a number with a spoofed automated voice response system that asks for your personal information, such as your credit card number (Vishing).



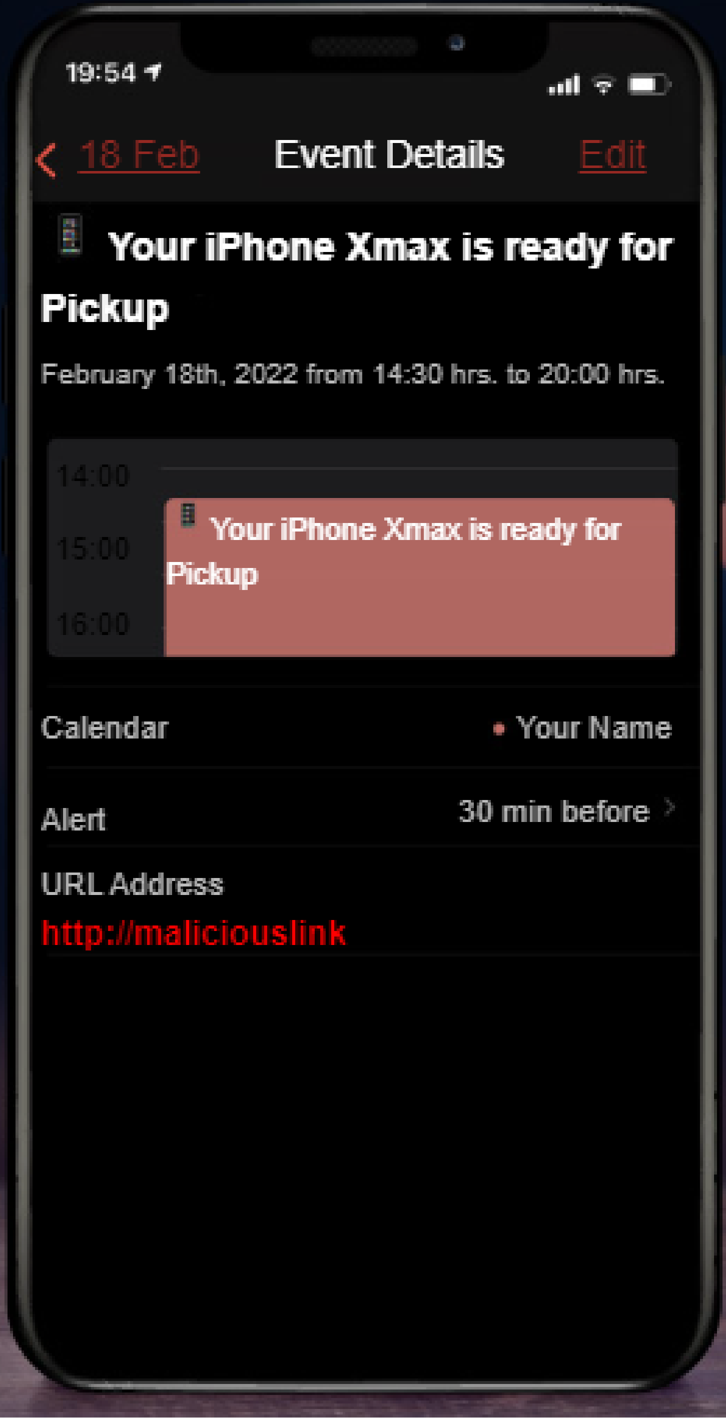
Text message Today 08:58

We have identified some unusual activity on your online banking. Please log in in via http://bit.do/dq3Wj to secure your account.

Calendar Phishing

Spammers will also target your calendar application, such as from Google, Microsoft, and Apple. Calendar invitations by default will appear on your calendar without your permission and can contain malicious links that can deliver malware to your computer or direct you to websites meant to steal your login credentials.

To avoid these types of scams, go to your calendar application's settings and disable events from being automatically added to your calendar. And avoid clicking on any links within or responding to suspicious calendar events or notifications.



Your iPhone Xmax is ready for Pickup

February 18th, 2022 from 14:30 hrs. to 20:00 hrs.

Calendar • Your Name

Alert 30 min before

URL Address
http://maliciouslink

Questions?

Rives Hassell-Corbiell
Cybersecurity Awareness
Program Manager
UTS | Tacoma Power | TPU

rhassellcorb@cityoftacoma.org
(253) 329-8471