Protect yourself from scams





Do you know how to spot a scam?

Pig Butchering Scams

Pig Butchering is a term or metaphor that describes a scam perpetrated over a long period of time to steal the victim's money repeatedly by online apps.

The term "Pig Butchering" references the practice of fattening a pig before the slaughter, these scams often involve fraudsters contacting individuals seemingly at random, then gaining trust before ultimately manipulating their targets and then disappearing with the funds.

- A slow build
- Sharpening the knife
- The slaughter

Don't trust that unexpected text or email from a stranger—it might be the first step in a "pig butchering" scam.

Be aware of all the signs. We will touch on several during this presentation to better educate you so that you will not be a victim.





Fake Websites & Online Shopping Scam

Legitimate looking websites are being created by scammers all the time.

Fake websites and social media ads can deceive consumers with sales but fail to deliver the promised goods or send counterfeit products.
This type of scam can also involve fake checkout processes which could result in financial loss or identity theft for the buyer.

Identifying a Fake Website

Fake websites are designed to steal your personal, financial, or login information. By checking specific details and looking for red flags, you can reduce the risk of falling victim to online scams.

1. Check the **domain name** carefully for misspellings, extra words, or unusual characters that mimic legitimate sites.
2. Inspect the site for **poor spelling, grammar, low-quality images, or awkward layouts** that legitimate companies usually avoid.
3. Be cautious of **deals that seem too good to be true**, especially steep discounts on high-value items.
4. Search for **independent user reviews** and check scam report sites like the Better Business Bureau's Scam Tracker.
5. Read the **shipping, return, and privacy policies** — missing or vague policies are suspicious.
6. Avoid sites that only accept **non-traditional payment methods** like gift cards, wire transfers, or cryptocurrency.
7. Run a **virus scan** if the site triggers excessive pop-ups or suspicious downloads.
8. Consider how you arrived at the site — links from unsolicited emails, texts, or ads are high-risk.
9. Check for a **complete and verifiable contact page** with a physical address and working phone number.

Pay close attention to detail. Never be too quick to click.





Irismicro
Sponsored ·

""This is my second pair. I only take them off to go to sleep. I put them on first thing in the morning. I am 59 and have neuropathy in my feet, they bring me comfort every day." -Lydia P.👍👍👍
❤️These orthopedic shoes provide great comfort and ease foot and knee pain! 😍
✅ Ideal for wide feet
✅ comfortable
✅ they are ideal for everyday life.
Get Yours Now"



irismicro

ALL SEARCH SHOPPING IMAGES

About 93,500 results

Including results for *iris*.
Do you want results only for irismicro ?

Iris
https://iristech.co › iris-micro

Iris micro - IrisTech

Iris micro is command line Iris. In order to make it acces
.sh files depending on your ...

iristech.app
https://www.iristech.app › page › iris-micro

Iris micro | Iris - iristech.app

Iris micro is command line Iris. In order to make it acces
.sh files depending on your ...

iristech.app
https://iristech.app › products › iris-micro

Iris micro | Iris

Made by Daniel Georgiev.



Tech Scam

The goal is to **steal money, sensitive information, or gain remote access** to devices.

Tech support scams trick victims into believing their computer, phone, or online account is compromised. Scammers impersonate legitimate companies like Microsoft, Apple, or banks, often using **phone calls, pop-ups, or phishing emails** to create panic. They may claim your system is infected with viruses, your account is at risk, or your personal information has been compromised. This could lead to victims providing control of their device and disclosing personal information.

Always be cautious of unsolicited contact, especially if it is unexpected. Hang up and call the company directly on a verified number. Avoid clicking on suspicious messages and **don't ever grant remote access to your device.**



Grandparent Scam

You receive a call or text message from someone claiming to be a grandchild or loved one asking for money or help with an emergency. They may claim to be incarcerated and need money for bail. They provide you with instructions on where to send the funds.

Hang up and call your loved one's phone directly.



IRS or Law enforcement scam

Scam artists are pretending to be an IRS official or an officer of the law. They will call claiming that you owe back taxes or that there is a problem with your tax return. They will also pose as Law enforcement and claim that you are in contempt of court. Scammers can even rig their caller ID to make the call look official. (Spoofing)

They will play on your fears.

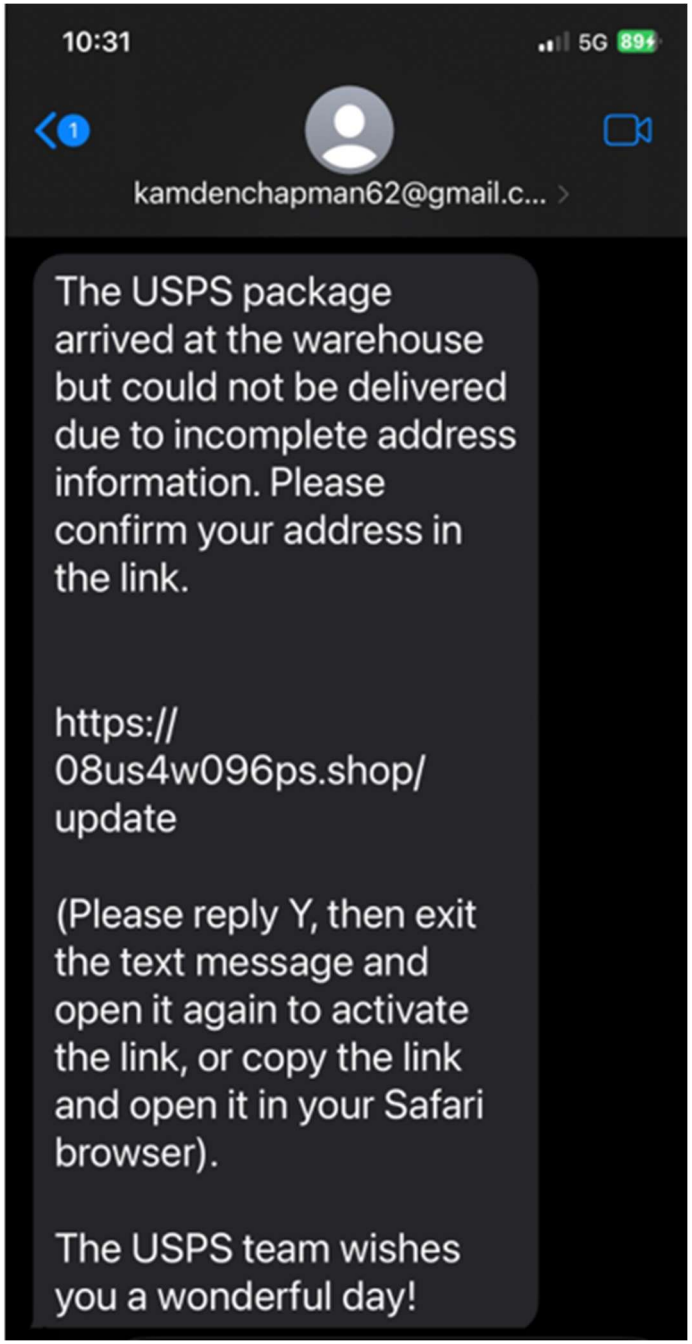
Law officials will never call you and demand money. Official claims will go through the court system with proper documentation.



Delivery Scams

You receive a text message stating that your package is undeliverable. It requires you to click on a link in order to update your information.

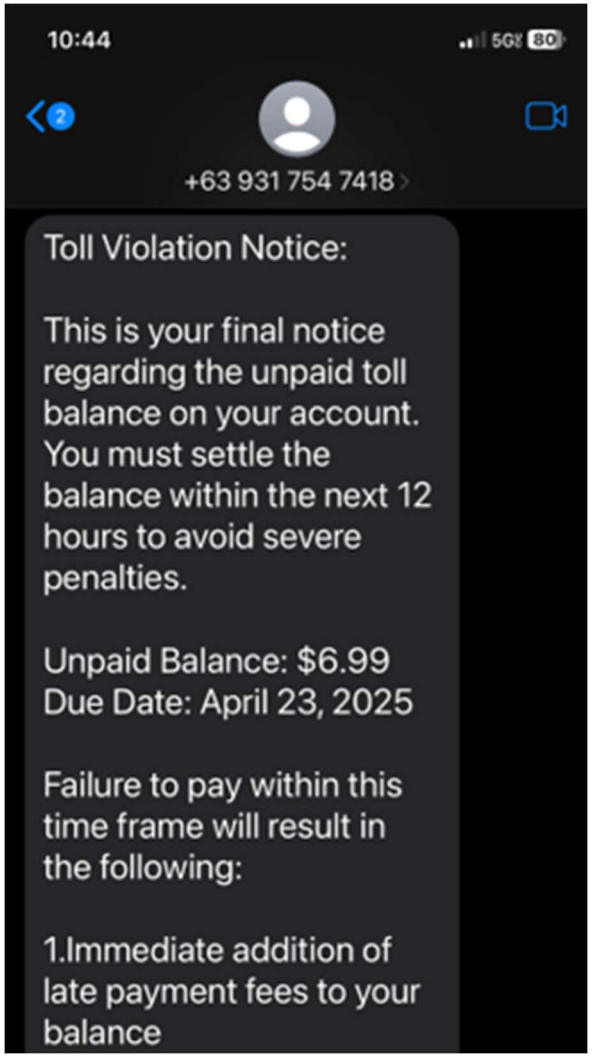
The *Post Office* does not have your cell phone number or your email address. If your package is undeliverable, they will leave a card in your mailbox.
If it is through *Amazon*, log back into your *Amazon* account and look for updates and messages. **Never click** on a text message link.

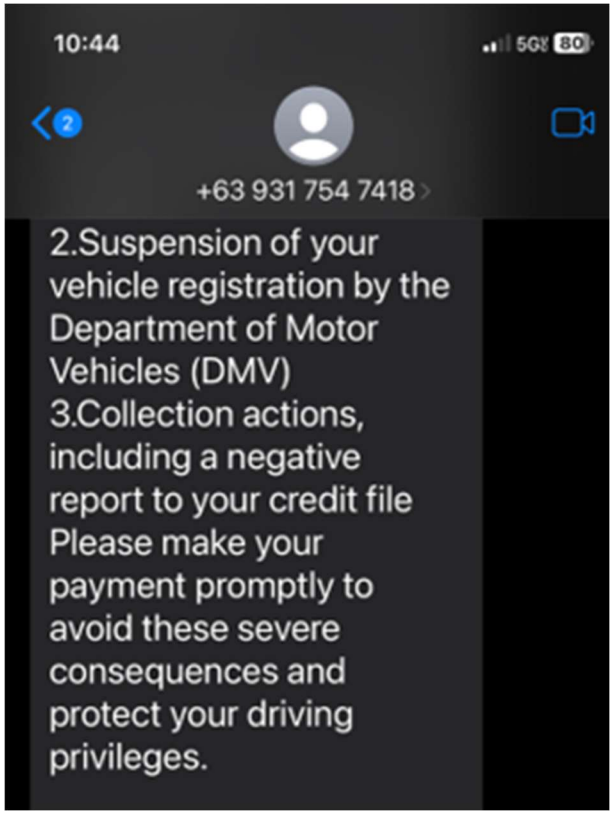

10:31
5G
89
1
kamdenchapman62@gmail.c...
The USPS package arrived at the warehouse but could not be delivered due to incomplete address information. Please confirm your address in the link.
https://
08us4w096ps.shop/
update
(Please reply Y, then exit the text message and open it again to activate the link, or copy the link and open it in your Safari browser).
The USPS team wishes you a wonderful day!

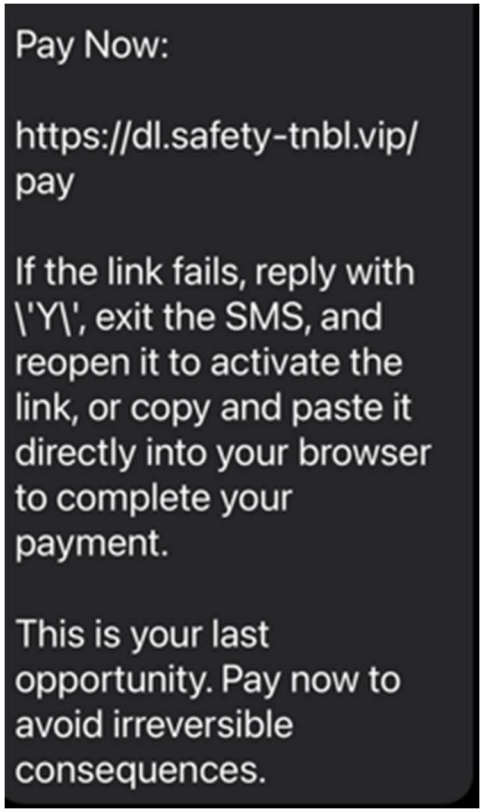


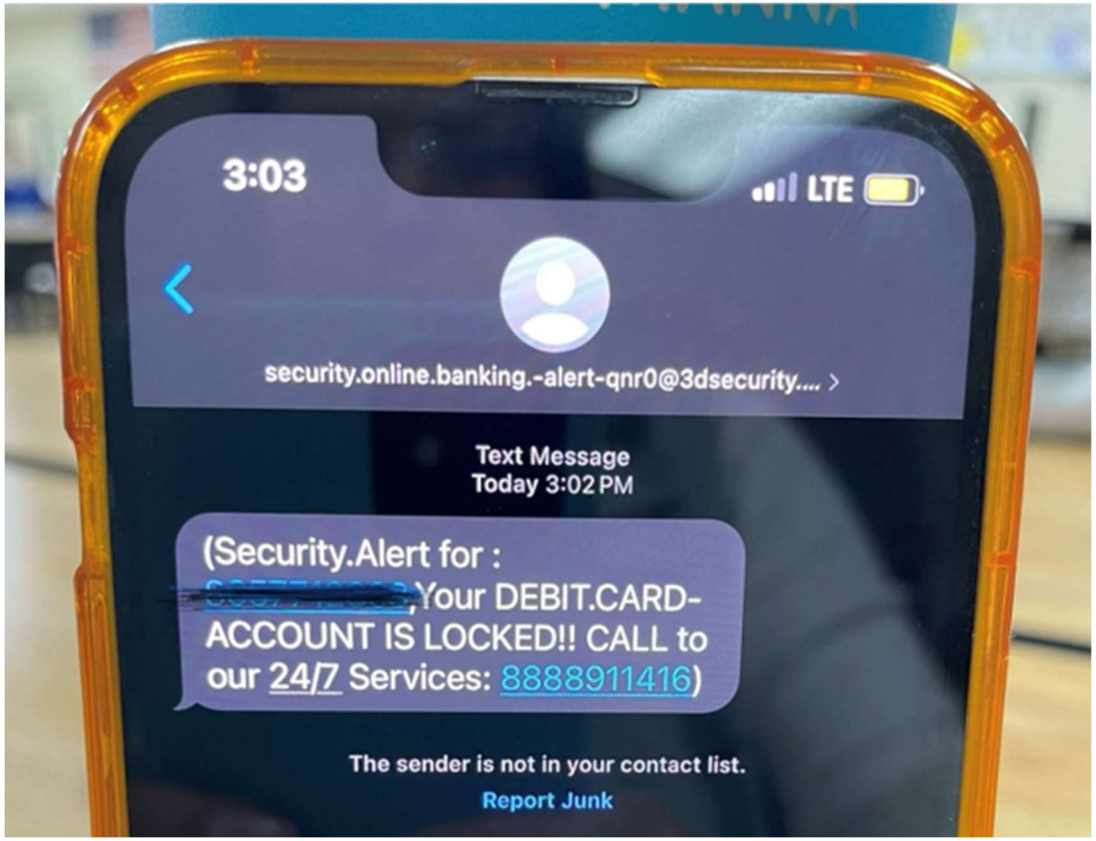
Scams communicated through Text messaging

If you do not know who is texting you, do not respond or click on anything that is provided. Scammers will impersonate your bank, your credit card company and even your post office. This is the first step in "making a connection" with you.

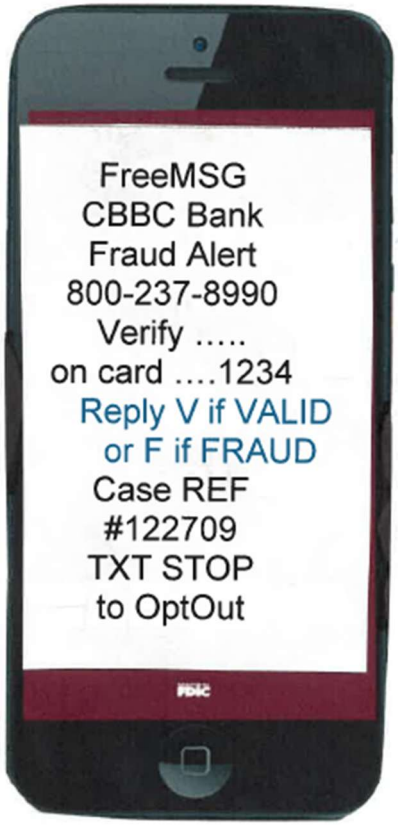

10:44
5G
80
2
+63 931 754 7418
Toll Violation Notice:
This is your final notice regarding the unpaid toll balance on your account. You must settle the balance within the next 12 hours to avoid severe penalties.
Unpaid Balance: $6.99
Due Date: April 23, 2025
Failure to pay within this time frame will result in the following:
1.Immediate addition of late payment fees to your balance


10:44
5G
80
2
+63 931 754 7418
2.Suspension of your vehicle registration by the Department of Motor Vehicles (DMV)
3.Collection actions, including a negative report to your credit file
Please make your payment promptly to avoid these severe consequences and protect your driving privileges.

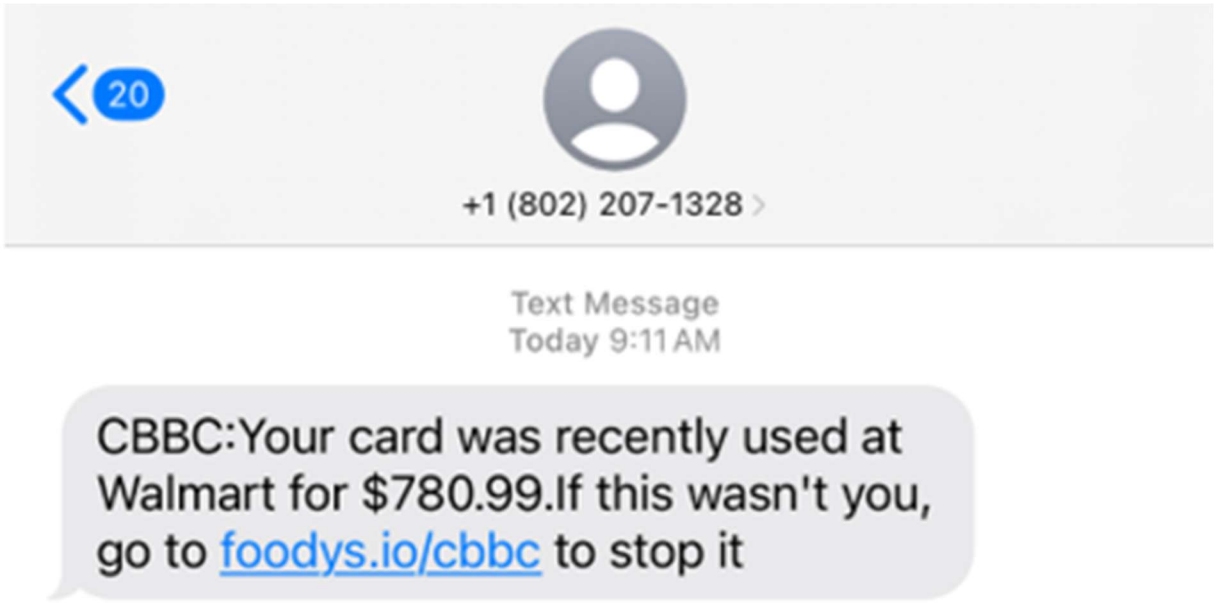

Pay Now:
https://dl.safety-tnbl.vip/pay
If the link fails, reply with \'Y\', exit the SMS, and reopen it to activate the link, or copy and paste it directly into your browser to complete your payment.
This is your last opportunity. Pay now to avoid irreversible consequences.



No bank is identified.



Actual Fraud Alert



This text attempts to identify the bank.

Take a closer look at where they are directing you.

Phishing

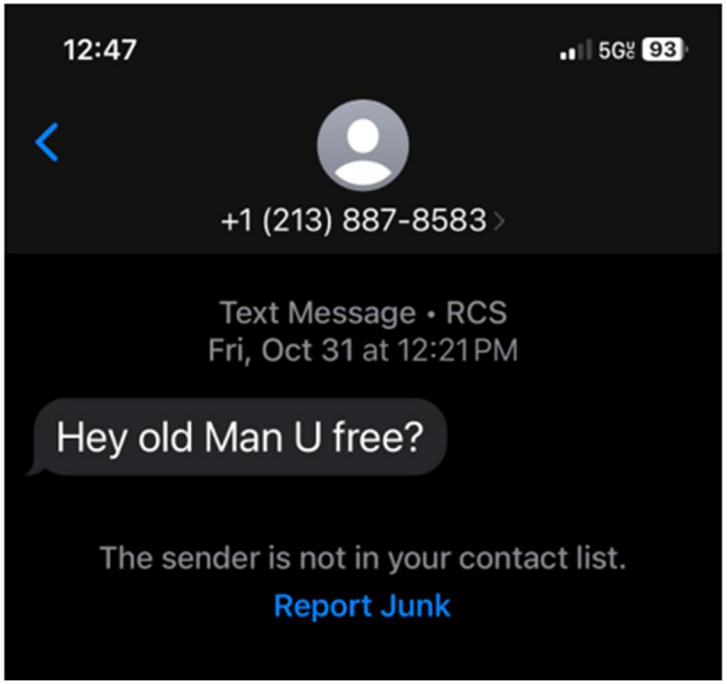
What is phishing?

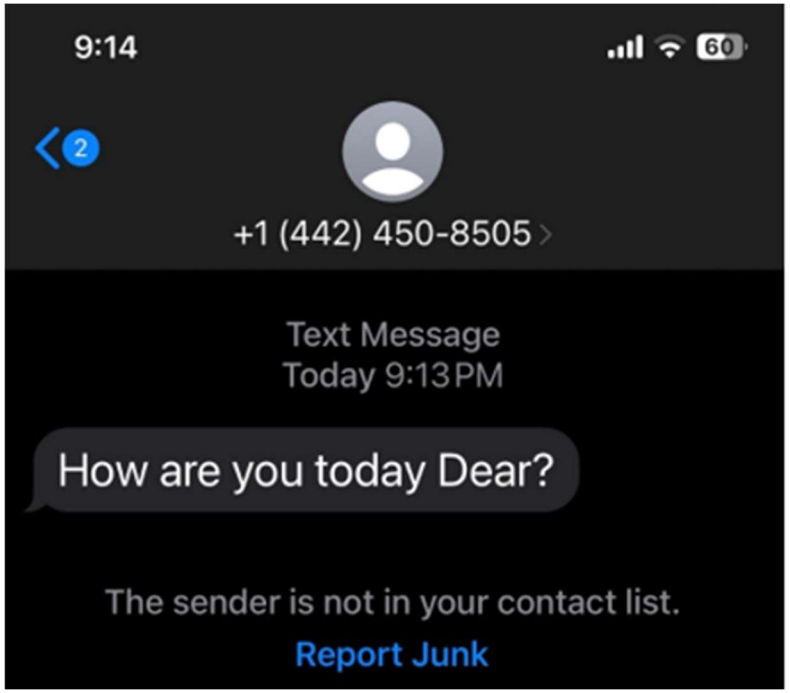
Phishing is a technique where attackers pose as trusted entities via email, text, or phone to trick victims into revealing sensitive data like passwords, credit card numbers, or installing malware. These scams rely on urgency or fear, directing users to fake websites to steal information.



Random Text Message - We all get them. Maybe it would be funny to reply. Maybe carry on with a conversation. I mean, it's just a random text, what harm could they do??

The truth is…….they can do a lot of harm, and you need to know why you should never engage.



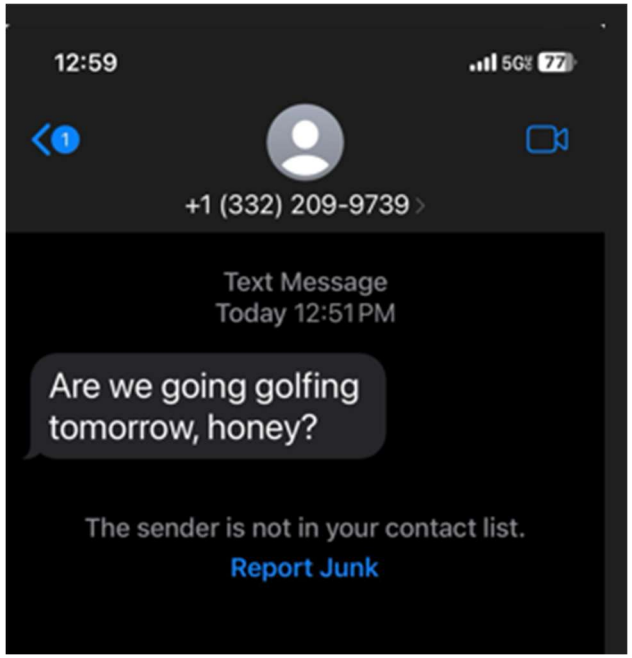


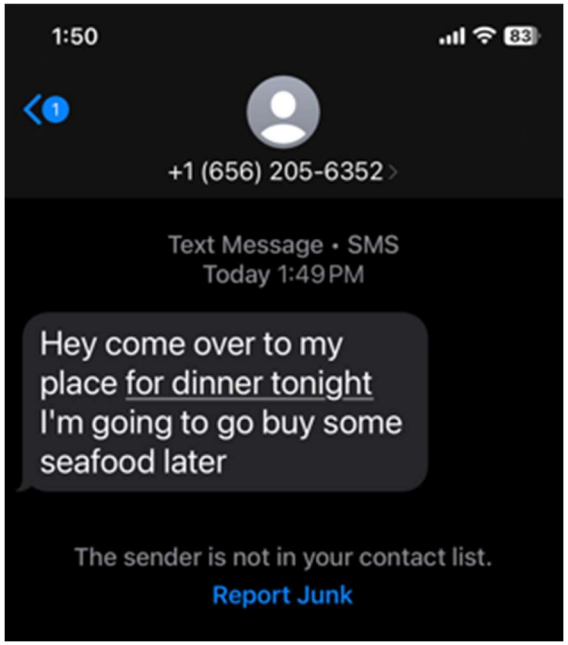
Random Text from an unknown number.

Trying to make a connection!

Random texts can expose you to scams, malware, privacy breaches, and unwanted contact — <u>simply engaging can confirm your number is active and increase your risk.</u>

Responding could develop into an “online” relationship for someone looking for a connection.
If a text comes from an unknown number, treat it cautiously — don’t click links, don’t share personal info, and only reply if you’re sure it’s legitimate.





(A slow build)

Dangers of Random Text Messages

How to Protect Yourself

- **Do not click** links or download attachments from unknown numbers.
- **Do not reply** to suspicious texts — it confirms your number is active.
- **Verify suspicious messages** by contacting the sender through official channels.
- **Block and report** unwanted or threatening texts via your carrier or app.

Bottom line: **Random texts can be harmless, but they can also be a gateway to serious security threats.** The safest approach is to treat them as potentially risky unless you know the sender.



Email Fraud

Email frauds (phishing) use deceptive messages to steal money or sensitive data by mimicking trusted sources. Common examples include urgent account suspension alerts (Netflix, banks), fake "updated invoice" payments, CEO fraud (business email compromise), and phishing links targeting credentials.

Look for urgent, threatening, or suspicious, misspelled sender addresses.

Common Examples of Email Frauds

- **Account Verification/Suspension Scam:** An email claiming to be from a company like Netflix, Amazon, or a bank stating, "Your account has been suspended" or "Your payment information is invalid," requiring you to click a link to log in and "fix" it.

- **The "Unexpected Invoice" Scam:** A fraudulent email with an attached invoice for a service you never ordered, attempting to get you to open a malicious attachment.

- **Package Delivery Failure:** A fake email claiming a parcel cannot be delivered, asking you to "click here" to update shipping information, which leads to a malware site.

- **Government Refund/Grant Scam:** An email claiming you are eligible for a tax refund or grant, designed to harvest your Social Security number or bank details.

- **Fake Invoice/Payment Request:** Criminals use "spoofed" email addresses that look almost identical to legitimate vendors, but with minor character changes, asking for payment to be sent to a new, fraudulent account.



Key Indicators of Fraudulent Emails

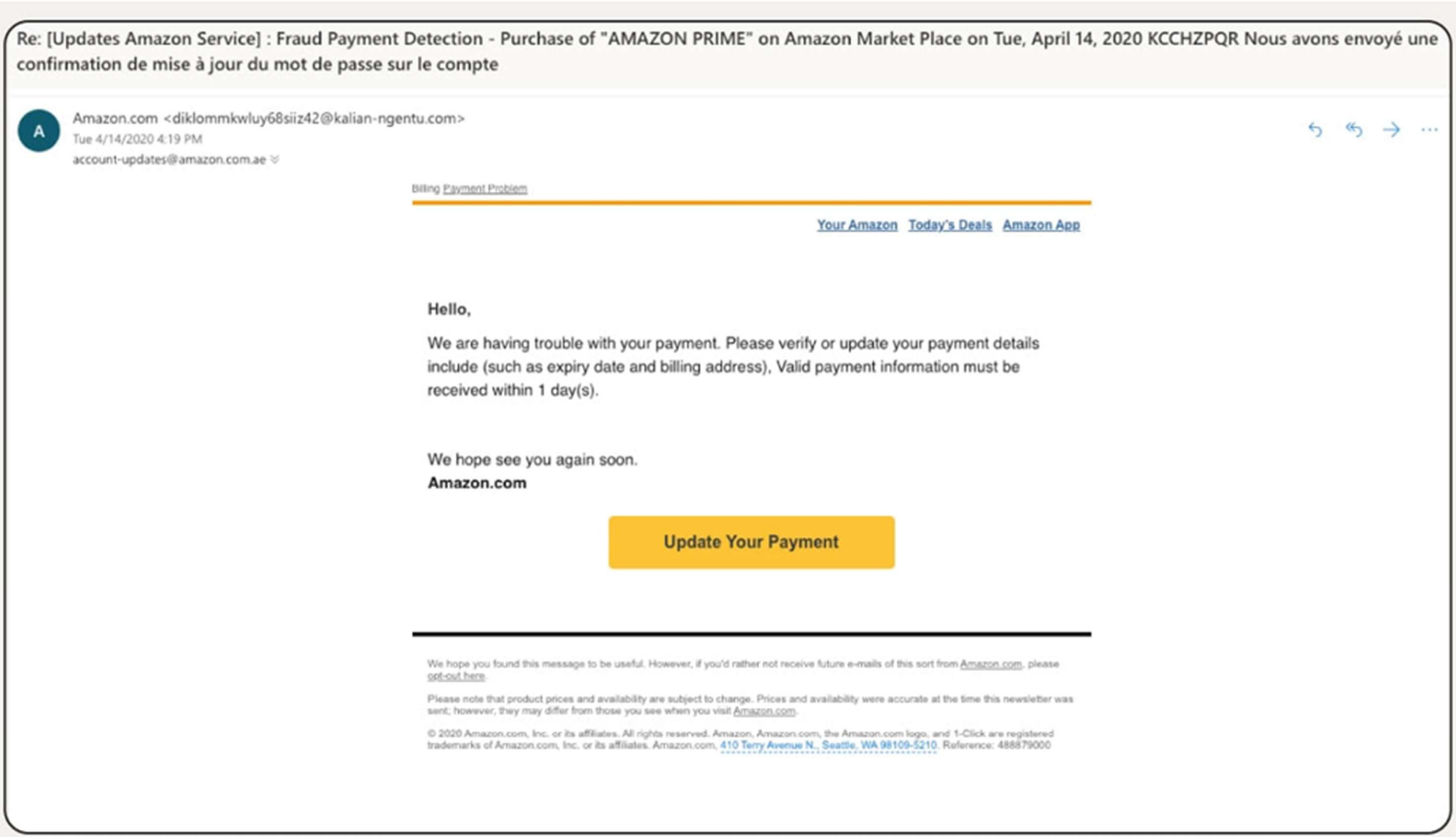
Sense of Urgency/Threats: "Action required," "Account will be closed in 24 hours," or "Immediate action needed".

Suspicious Links/Attachments: Hover over links before clicking to see the real destination, and avoid opening unexpected documents.

Generic Greetings/Poor Grammar: Instead of your name, they use "Dear Customer" or have multiple spelling mistakes.



Mismatch in Sender Address: The display name says "CBBC Bank" but the actual email address is a random, unrelated string (e.g., xyz123@gmail.com).



Re: [Updates Amazon Service] : Fraud Payment Detection - Purchase of "AMAZON PRIME" on Amazon Market Place on Tue, April 14, 2020 KCCHZPQR Nous avons envoyé une confirmation de mise à jour du mot de passe sur le compte

A

Amazon.com <diklommkwluy68siiz42@kalian-ngentu.com>
Tue 4/14/2020 4:19 PM
account-updates@amazon.com.ae

Billing Payment Problem

Your Amazon Today's Deals Amazon App

Hello,

We are having trouble with your payment. Please verify or update your payment details include (such as expiry date and billing address), Valid payment information must be received within 1 day(s).

We hope see you again soon.
Amazon.com

Update Your Payment

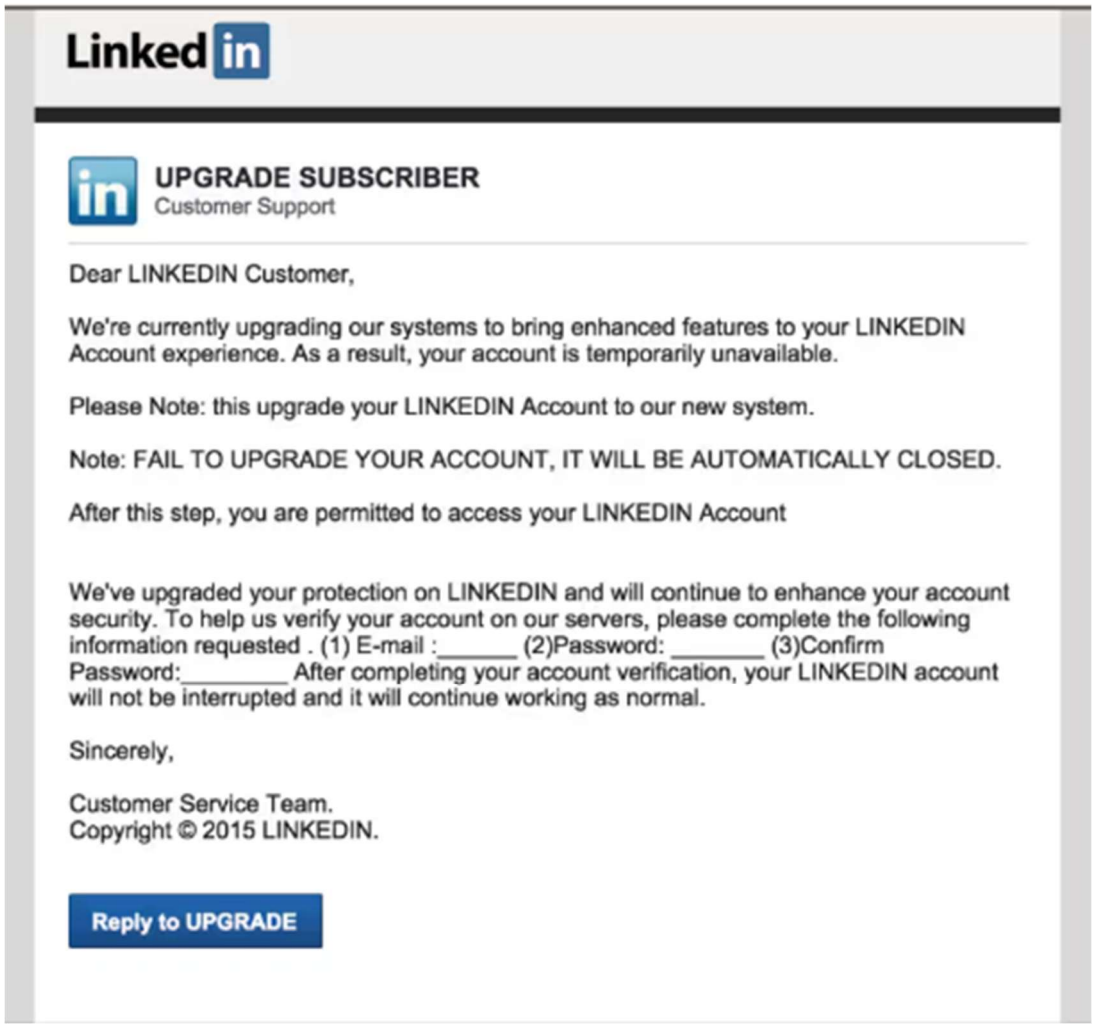
We hope you found this message to be useful. However, if you'd rather not receive future e-mails of this sort from Amazon.com, please opt-out here.

Please note that product prices and availability are subject to change. Prices and availability were accurate at the time this newsletter was sent; however, they may differ from those you see when you visit Amazon.com.

© 2020 Amazon.com, Inc. or its affiliates. All rights reserved. Amazon, Amazon.com, the Amazon.com logo, and 1-Click are registered trademarks of Amazon.com, Inc. or its affiliates. Amazon.com, 410 Terry Avenue N., Seattle, WA 98109-5210. Reference: 488879000

How to tell this is a phishing email:

This Amazon phishing email comes from a suspicious email address, doesn't include the customer's name, and pressures the customer to update their payment information quickly.


Linked in
UPGRADE SUBSCRIBER
Customer Support
Dear LINKEDIN Customer,
We're currently upgrading our systems to bring enhanced features to your LINKEDIN Account experience. As a result, your account is temporarily unavailable.
Please Note: this upgrade your LINKEDIN Account to our new system.
Note: FAIL TO UPGRADE YOUR ACCOUNT, IT WILL BE AUTOMATICALLY CLOSED.
After this step, you are permitted to access your LINKEDIN Account
We've upgraded your protection on LINKEDIN and will continue to enhance your account security. To help us verify your account on our servers, please complete the following information requested . (1) E-mail :_____ (2)Password: _____ (3)Confirm Password:_____ After completing your account verification, your LINKEDIN account will not be interrupted and it will continue working as normal.
Sincerely,
Customer Service Team.
Copyright © 2015 LINKEDIN.
Reply to UPGRADE

How to tell this is a phishing email:

In this LinkedIn scam, the user's name isn't specified in the greeting, which means it's likely sent to multiple email addresses in bulk. The business name is in all capital letters throughout the email, which is not their trademark or branding. There are multiple grammar issues, which is uncommon for a reputable organization. LinkedIn will also never ask you for your password via email.

Here's your invoice

ORDER DATE

Thursday, 03 July 2025

ORDER NUMBER

OD42315415

SHIPPING METHOD

FedEx Standard Overnight

SHIPMENT DATE

Friday, 04 July 2025

Your payment of **$716.00** for the purchase of an **Apple iPhone 15 (128 GB)** has been successfully processed. To review the transaction details, please log in to your PayPal account. A detailed receipt has been automatically sent to your registered email address. If you have any questions, please contact us for assistance. Thank you for your purchase.

Order Summary

Product	Qty	Description	Amount
iPhone Apple iPhone 15 (128GB) - UNLOCKED Variant Code: 9ZCGOXKM9PFS	1	Apple iPhone 15 (128GB) features a **6.1-inch Super Retina XDR display**, a **48MP main camera** with advanced photography capabilities, and the **A16 Bionic chip** for smooth performance.	$679.99
		Subtotal	**$679.99**
		Tax (5.3%)	**$36.01**
		Total	**$716.00**

Payment Information

Method	Details	Amount
Auto-Debit	Payment processed successfully	$716.00

Payment Information

Method	Details	Amount
Auto-Debit	Payment processed successfully	$716.00

Fraud Alert: If this activity was not initiated by you, please contact us immediately at **+1 (828) 316-6371** to report the incident.

Bank Processing Information

Financial institutions typically require 1-3 business days to process transactions. The posted date in your bank account may differ from the transaction date shown here. For immediate verification, please reference the authorization code: **9ZCGOXKM9PFS**.

Premium Support Team

+1 (810) 246-5684

Availability

24/7 Support

E-Receipt Sent to

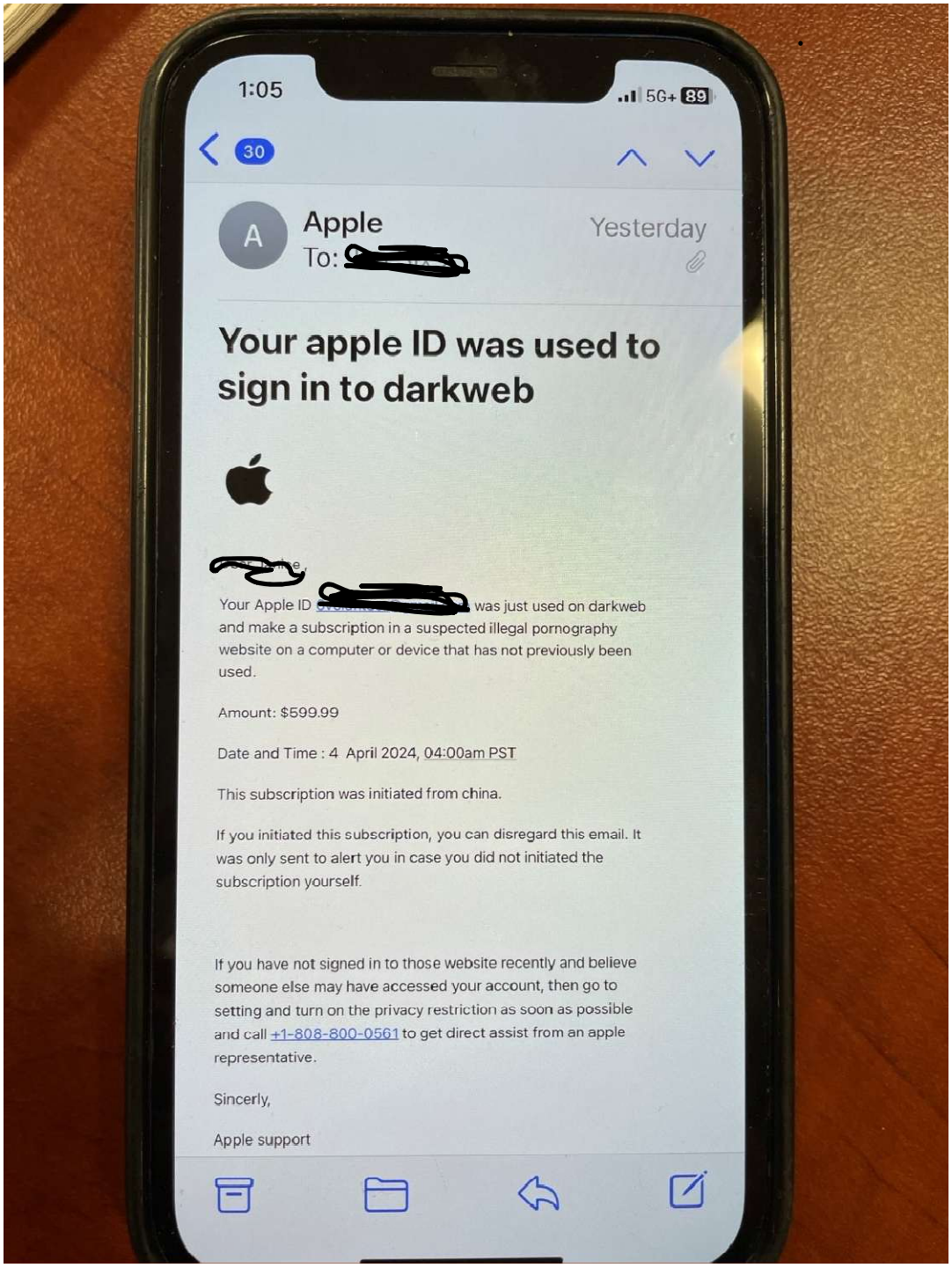
bethpyle28@gmail.com

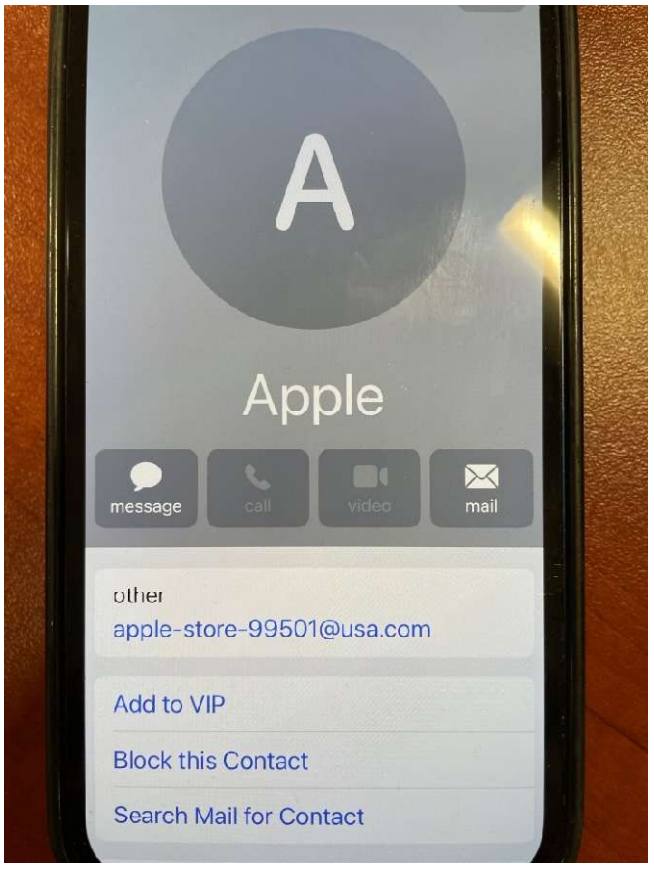
Help & Contact | Security | Apps

PayPal is committed to preventing fraudulent emails. Emails from PayPal will always contain your email address. Learn to identify phishing

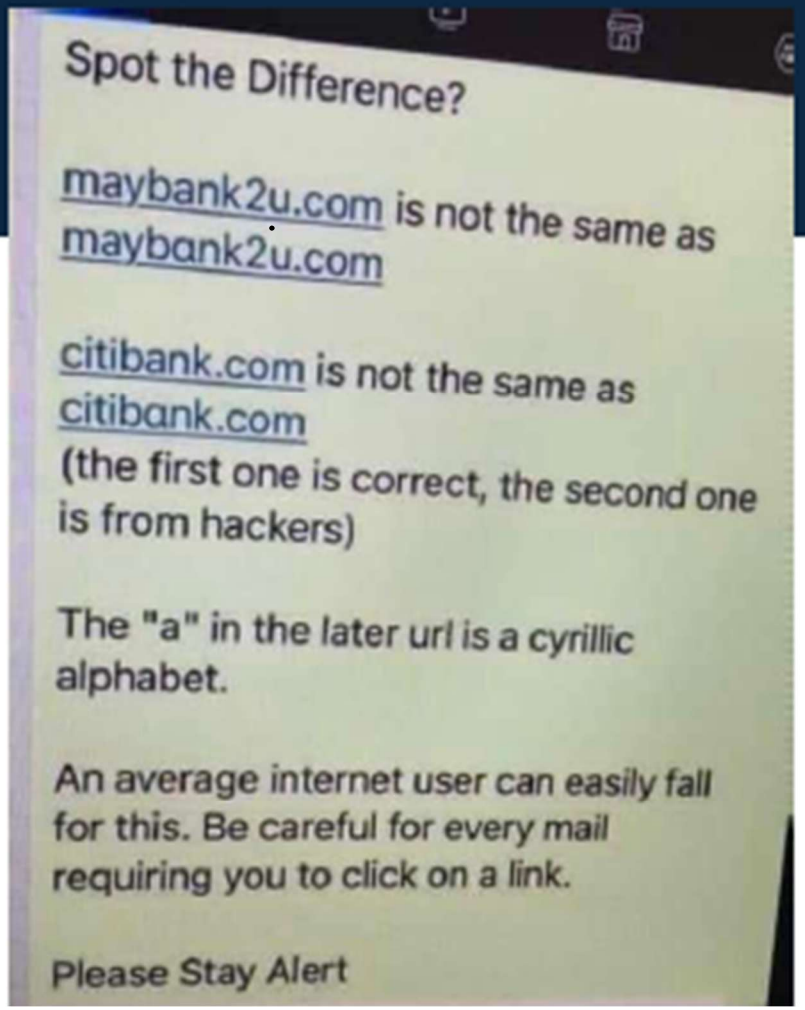
Please do not reply to this email. We are unable to respond to inquiries sent to this address. For immediate answers, visit our Help Centre.

2025 PayPal, Inc. All rights reserved. PayPal is a registered trademark of PayPal, Inc.


1:05
5G+ 89
30
A
Apple
To: [redacted]
Yesterday
Your apple ID was used to sign in to darkweb
Dear [redacted],
Your Apple ID [redacted] was just used on darkweb and make a subscription in a suspected illegal pornography website on a computer or device that has not previously been used.
Amount: $599.99
Date and Time : 4 April 2024, 04:00am PST
This subscription was initiated from china.
If you initiated this subscription, you can disregard this email. It was only sent to alert you in case you did not initiated the subscription yourself.
If you have not signed in to those website recently and believe someone else may have accessed your account, then go to setting and turn on the privacy restriction as soon as possible and call +1-808-800-0561 to get direct assist from an apple representative.
Sincerly,
Apple support


A
Apple
message
call
video
mail
other
apple-store-99501@usa.com
Add to VIP
Block this Contact
Search Mail for Contact

Spot the Difference





Romance Scams

Be wary of relationships formed online, especially if they are asking for financial support. Don’t give out any private details.

Red Flags and Tips review

Be wary when given pressure to act immediately. Use of scare tactics, telling you a loved one is in danger, that your computer has been hacked or threatening arrest if you don't act now.

Below are common warning signs of a phone scam:

- A claim that you have been specially selected.
- Use of high-pressure sales tactics and “limited time” offers.
- Reluctance to answer questions about the business or the offer.
- Request that you “confirm your personal information.”
- Realize that numbers can be spoofed.

Avoiding Scams and Scammers

- Do not open email from people you don't know. ...
- Do not open text messages from people you don’t know.
- Be careful with links and new website addresses. ...
- Secure your personal information – never give it out.
- Stay informed on the latest cyber threats. ...
- Use Strong Passwords.

Red Flags and Tips review

Thoroughly inspect any message and ask yourself these questions:

- Does it push urgency?
- Does it contain threatening language?
- Does it make unrealistic promises?
- Does it contain suspicious links or attachments?
- Do I recognize the sender?

Review the address of the sender.

Look for misspelled words.

It's very easy to copy a company logo or to send messages from an address that looks legitimate. It's even easy to spoof phone numbers of legitimate businesses.

Always be on your guard. Criminals will use every means possible to make contact. This contact attempt could come from your email, a text message, a phone call or even a simple compliment on social media.



If you are a victim or need a resource:

IC3.GOV

The Internet Crime Complaint Center (IC3) is the central hub for reporting cyber-enabled crime. It is run by the FBI, the lead federal agency for investigating crime.

In conclusion, ...

The best way to deal with a scammer is to completely ignore them. Scammers want things from others, and they want to steal things. If you ignore them, they don't get what they want, they will eventually give up.

Federal law says banks must reimburse you for unauthorized transactions, but they don't for authorized ones. So, if you voluntarily give someone money, that's on you.

Stay vigilant against scams and safeguard your personal information.
Be wary of any unexpected calls, messages, emails or texts.
Always double check the legitimacy of requests before acting.
Trust your gut – if something feels off, it’s always better to double check.



If it sounds too good to be true,
it probably is.

CBBC Bank

Thank you for attending. We hope that this presentation has been insightful and provided you with important information to help keep you and your finances safe.



Beth Pyle
Senior Vice President
Information Security Officer
(865) 977-5906
bpyle@cbbc.bank

Laura Lenear
Vice President
Marketing Director
(865) 379-2509
llenear@cbbc.bank

Jonathan Settlemire
Senior Vice President
Chief Operations Officer
(865) 379-2506
Jsettlemire@cbbc.bank