CBBCBank

Common Scams and How to Avoid Them

Thursday, October 17th | 10 am

1

Agenda

- What is a Scam?
- What types of Scams exist?
- How to protect yourself
- Resources

2

What is a Scam?

scam
[skam]

noun *informal*

a dishonest scheme; a fraud:
"an insurance scam"

Similar: fraud | swindle | racket | trick | diddle | fraudulent scheme

verb

swindle:
"a guy that scams the elderly out of their savings"

*Source: Oxford Languages

3

Do you know how to spot a scam?

This seminar is to help make you aware of the latest scams and protect your money and personal information from potential scammers.

4

Question

Which scam is the top priority of FBI, Interpol, and MI6?

Answer: Pig Butchering

5

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 into phony investments, and then disappearing with the funds.

6

Pig Butchering (contd.)

How it occurs

- A slow build
- Sharpening the knife
- The slaughter

Don't trust that unexpected text, social media message, or email from a stranger – it might be the first step in a "Pig Butchering" scam!

7

Pig Butchering (contd.)

Who conducts pig butchering?

Scam Centers

Thailand
Vietnam
Philippines
United States of America (Alabama, Ohio, Michigan, California…)

8

Pig Butchering (contd.)

9

Pig Butchering (contd.)

- **Compounds Street Level**

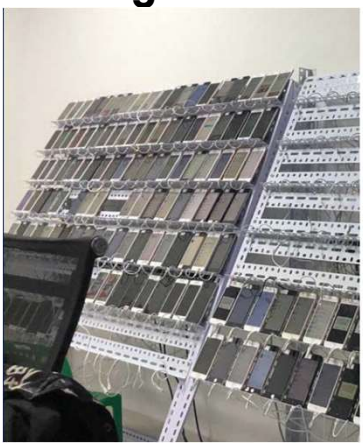
Heavily guarded entrances

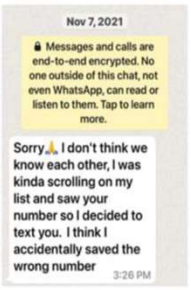
Razor wire around the compound

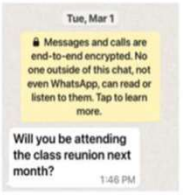
10

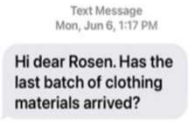
Pig Butchering (contd.)

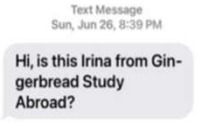
Initiating Contact









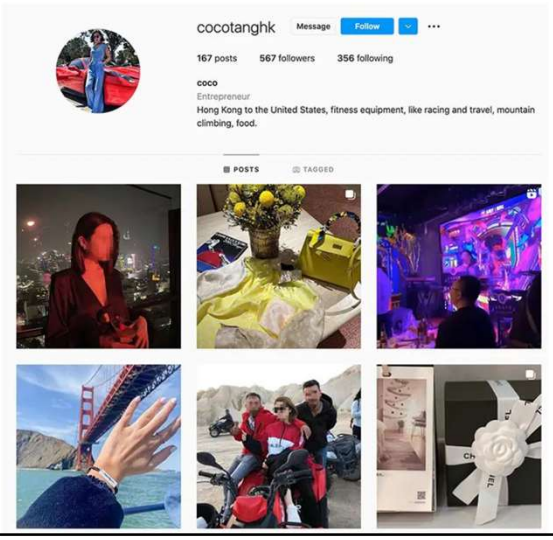


11

Pig Butchering (contd.)

Building Trust

- Continues Conversation
- Talks about living a life of luxury – trips to Europe, buying jewelry, etc.
- Directs victims to Social Media pages

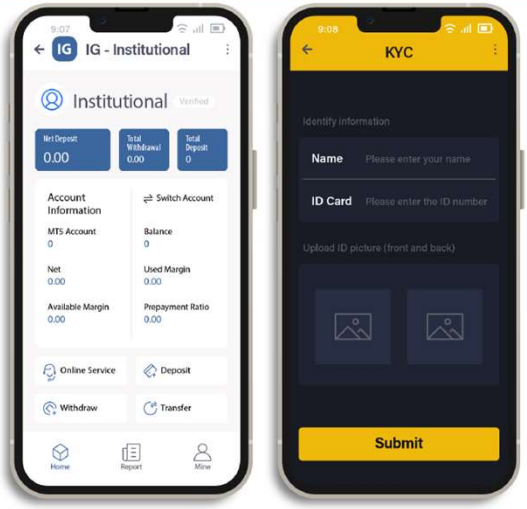


12

Pig Butchering (contd.)

Introducing Investments

- Proves to victim that they have mainstream crypto in their own app.
- Shows their own portfolio.



13

Pig Butchering (contd.)

Prompting Deposits

- The fattening

14

Pig Butchering (contd.)

Manipulates Further Investments

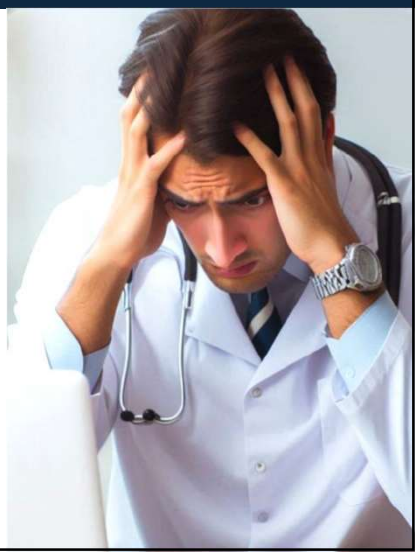
- Makes investments seem too good to be true.
- Victims put more money into the scam.

15

Pig Butchering (contd.)

Butchered/Killed

- Victim runs out of money to deposit
- Scammer disappears forever



16

Pig Butchering (contd.)

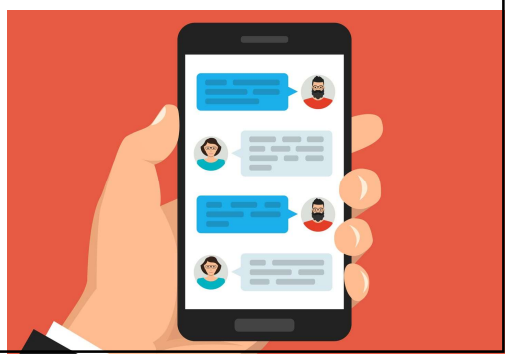
Who are the most vulnerable?

- The Wealthy
- The Lonely
- Males (80% of victims)

17

Text Messaging

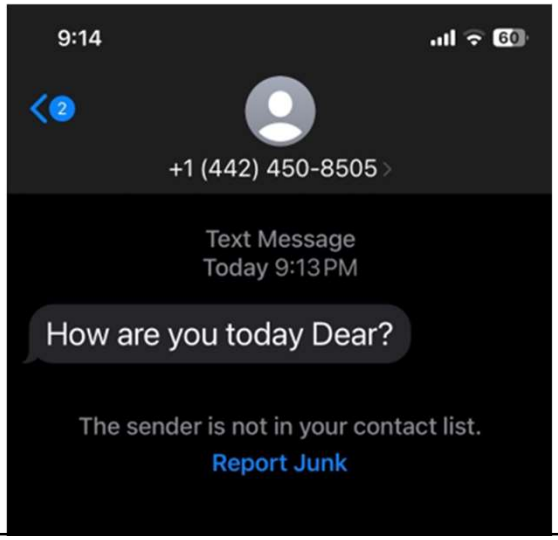
If you do not know who is texting you, **do not respond or click on anything that is provided**. Scammers will impersonate your bank, your credit card company, Vendors you may use or even your post office. This is the first step in "making a connection" with you.



18

Text Messaging - Example

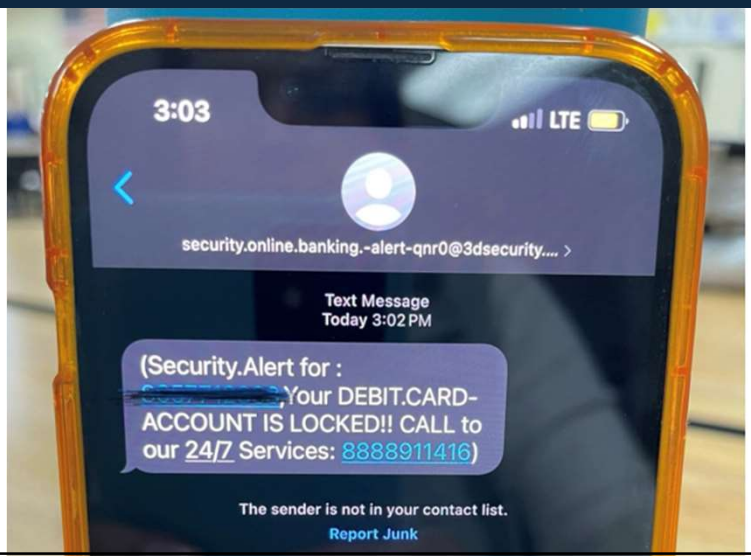
Random Text from an unknown number trying to make a connection.



19

Text Messaging - Example

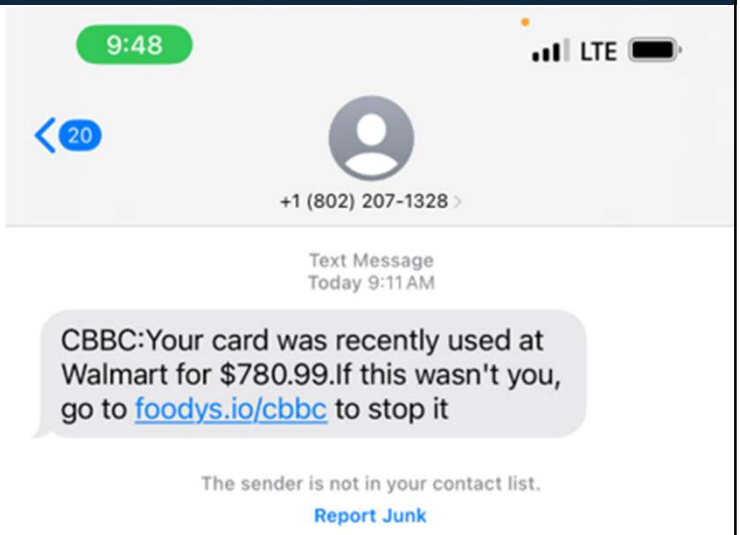
There is no Bank Identification.



20

Text Messaging - Example

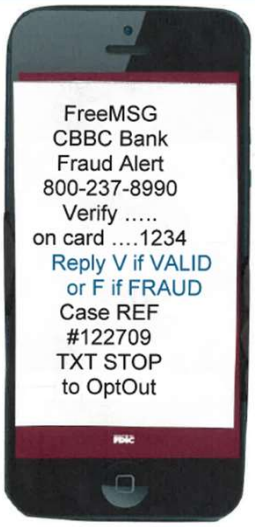
This text attempts to identify the bank. Take a closer look at where they are directing you.



21

Text Messaging - Example

Actual Bank Text Message from CBBC Bank.



22

Phone Scams

We have seen an increase in telephone and text scammers posing as CBBC Bank employees and asking for our customers' personal information. Remember, CBBC Bank will **NEVER** call and ask for sensitive information because we already have it.

23

24

Cryptocurrency Scams

Scammers may also impersonate new or established businesses offering fraudulent crypto coins or tokens with promises of high returns. They might create slick social media ads, news articles, or websites to look legitimate and trick new investors into buying. These fake investment opportunities may require high up-front fees that supposedly get invested in crypto but actually go directly into the scammer's pocket.

You might be asked to wire money to an online cryptocurrency company. You are coerced into opening an account with this company and then wire money to fund the account.

You may be asked to withdraw your money and deposit it at a local Bitcoin ATM.

25

Cryptocurrency Scams (contd.)

Scammers are the only ones who will ask them to withdraw cash and enter it into a local bitcoin ATM – not Microsoft, law enforcement, a banking regulator saying the bank is about to fail, an attorney, a legitimate romantic interest nor a friend with a great investment opportunity.

Scammers will convince their victims to lie to anyone who asks questions – especially bankers.

26

Cryptocurrency Scams (contd.)

Question any appealing investment offers that guarantee huge returns. Before sending any money, look up the business at trustworthy resources online to verify if it's legitimate. Again, you should never be pressured when it comes to your money.

27

Gift Card Scam

Some scammers impersonate government agencies, financial institutions or businesses claiming that you need to make urgent payments with a gift card, or you'll face legal action. By creating this false sense of urgency, they pressure you into buying expensive gift cards and sharing the numbers on the back.

Businesses and government agencies will never ask you to purchase gift cards for payments. Never give the number on the back of a gift card to anyone you don't know.

28

Marketplace Scam

When responding to ads or interacting in marketplaces on social media, research sellers and products independently to make sure it is legit.

Know the red flags such as “too good to be true” or a buyer that redirects you to a different site or asks for personal information. Maybe they “accidently” overpaid you and requests that you return the overage through means such as cashier check, gift cards, etc.

29

Online Shopping Scam

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.

30

Tech Scam

Pop-up messages, cold calls or emails are tactics uses by scammers posing as tech support. Their goal is to deceive users into believing that their computer has issues or has been hacked. 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.

31

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.

32

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.

33

IRS or Law Enforcement Scam (contd.)

No law enforcement agency tells you when you are going to be arrested. They just show up with a warrant in hand.

34

Lottery Scam

You receive a request to prepay fees or taxes to receive a large prize you supposedly won.

- Reject any offer that asks you to pay for a "prize" or "gift."
- If you receive a letter offering you a large sum of money for little effort other than sending a "processing" fee.

35

Charity Scam

You receive a request to donate to a charity that you have never heard of and for which you cannot find an official website.

36

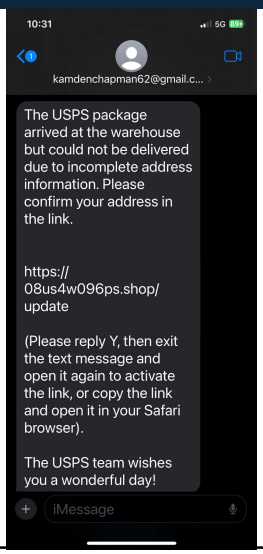
Post Office Scam

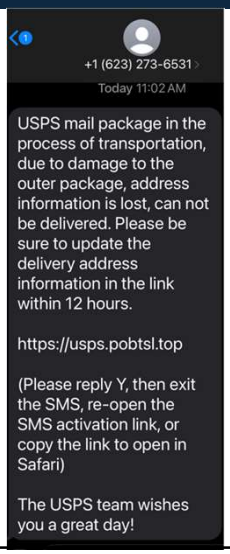
You receive a text message stating that your package is undeliverable. It requires you to click on a link in order to update your information.

The Post Office does not have your cell phone number. If your package is undeliverable, they will leave a card in your mailbox.

37

Post Office Scam – Examples



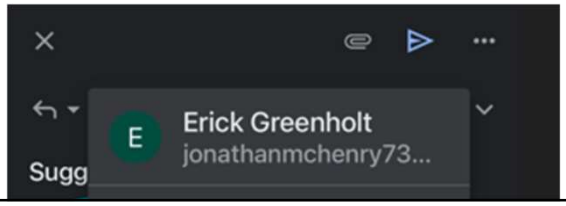


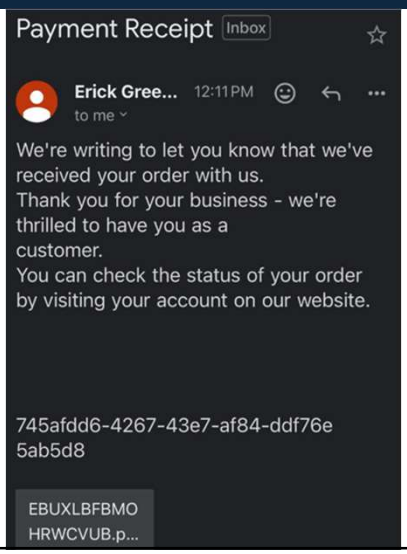
38

Email Scams

Whenever you receive an email from someone you don't know, delete it.

As you can see, by clicking on the return address, this email doesn't reflect any kind of business.





39

Amazon Scams

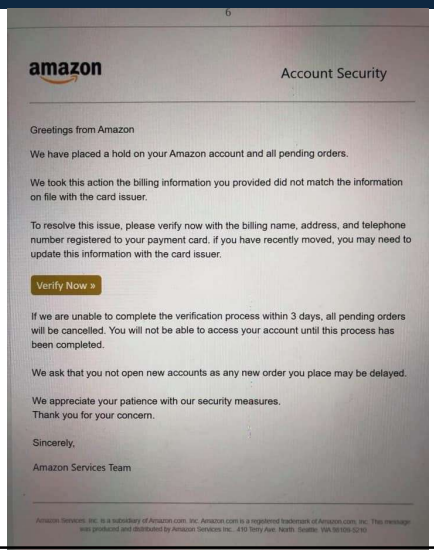
Amazon will never ask you to install an app or download software in order to receive a refund or get customer service help.

Amazon will never ask you to pay over the phone or provide any payment information.

Amazon will never ask you for your account information or passwords.

Log back into your Amazon account and look for updates and messages. **Never click on a text message link.**

Always verify your orders, account, messages INSIDE of your Amazon online account.



40

Check Cashing Scam

In the past, cashier's checks were considered just as good as cash. However, lately many consumers have become victims of scams involving a fraudulent cashier's check. Counterfeiters have become very good at reproducing bank checks, and it is often very difficult to detect fraudulent cashier's checks.

41

Common Cashier's Check Scams

Selling Goods -You offer goods for sale in the marketplace, through a newspaper ad, or over the Internet. A buyer sends you a cashier's check for the agreed-upon price. The cashier's check turns out to be fraudulent.

42

Common Cashier's Check Scams

Overpayments - This is a variation of the selling goods scam. You're overpaid for an item you advertised in the classifieds or in an online auction. The buyer either claims they sent the wrong amount by "mistake," or they explain that they paid more than the purchase price to satisfy their obligations to you and a third party with a single check. They ask you to deposit the check into your account and wire transfer some or all of the excess to them or a third party. The cashier's check turns out to be fraudulent.

43

Common Cashier's Check Scams

Sudden Riches - You receive a cashier's check and a letter that you've won a foreign lottery or inherited money. The letter will state that you have to pay a fee – a processing fee or a fee to cover taxes – before you receive the money. The cashier's check is enclosed to cover that fee. The letter asks you to deposit the cashier's check into your account and wire the fee to a third party. The cashier's check turns out to be fraudulent.

44

Common Cashier's Check Scams

Mystery Shopping – You receive a letter informing you that you have been chosen to act as a "mystery" or "secret" shopper. The letter includes a cashier's check, and you are told to deposit the check into your account. You're instructed to use a portion of the deposited funds to purchase merchandise at designated stores, transfer a portion of the funds to the sender or a third party, using a designated wire service company, and keep the remainder. The cashier's check turns out to be fraudulent.

45

Common Cashier's Check Scams

Regardless of the pitch, the result is the same: The result of these scams is that the fraudulent check will be returned to the bank unpaid. The bank will then deduct the amount of the check from your account or otherwise seek repayment from you. Either way, you have lost items, money, or both.

46

Tips for Avoiding Cashier's Check Fraud

Try to know the people with whom you do business. Be cautious about accepting checks – even a cashier's check – from people you do not know, especially since it may be difficult to pursue a remedy if the transaction goes wrong.

47

Tips for Avoiding Cashier's Check Fraud

When you use the Internet to sell goods or services, consider other options, such as escrow services or online payment systems, rather than payment by a cashier's check.

48

Tips for Avoiding Cashier's Check Fraud

If you do accept a cashier's check for payment, never accept a check for more than your selling price if you are expected to pay the excess to someone else.

49

Tips for Avoiding Cashier's Check Fraud

If you want to find out whether a cashier's check is genuine, call or visit the bank on which the check is written.

50

Tips for Avoiding Cashier's Check Fraud

Be wary of taking action before you can be sure that the payment you received is good.

51

Tips for Avoiding Cashier's Check Fraud

Be suspicious if someone pressures you to act quickly before you know the payment you received is good.

52

Check Fraud – WASHING!

Criminals use common household products like nail polish remover or bleach to remove the ink from a check, replace the value with a higher amount, and/or replace the payee.

53

Check Fraud – WASHING!

- Avoid using paper checks, and instead make online payments or use peer-to-peer apps
- Have BankOnLine with your Financial Institution
- Set up transaction alerts to monitor your checking account
- If you do send a check by mail, take it directly to the post office
- Ask the recipient to notify you when they receive the check
- Write checks with a black gel ink pen

54

Check Fraud – WASHING!

BankOnLine is one of the most important tools for protecting your account.

55

Romance Scams

Be wary of relationships formed online, especially if they are asking for financial support, need money to come visit you or simply want to surprise you with an elaborate gift with your assistance.

56

Fake Rental Scams

Be cautious of houses for sale or rent or vacation properties listed online. Scammers will set up a fake website and list these properties. You send your first month's rent, payment, or deposit to someone pretending to be the owner.

Always use official sites. If you use VRBO or AIRBNB, make sure you have an account and can personally log into the site to search properties.

57

Puppy Scams

Scammers will post fake litters online or pretend to be an existing breeder to take advantage of those looking to purchase a pet.

They will ask for money upfront through a cash app in order to proceed.

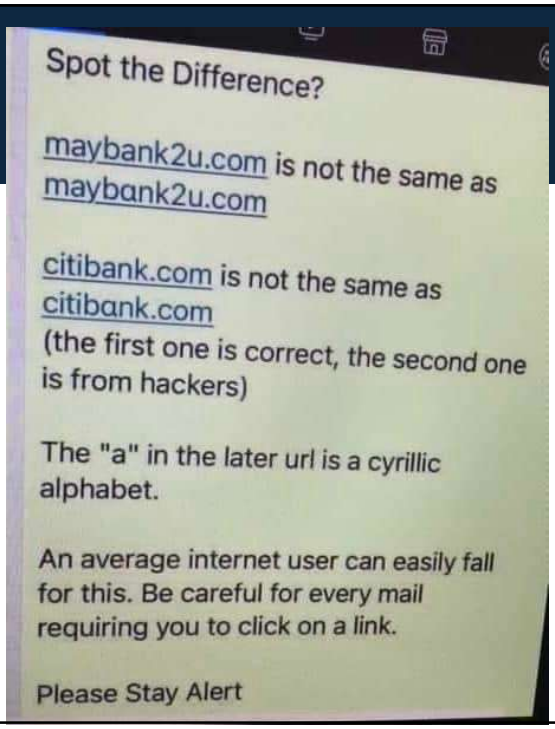
58

Fake Websites

Legitimate looking websites are being created by scammers all the time. A quick look at Google search will lead you to a real looking phone number. When you call, they will try to obtain your sign on details or other personal information.

59

Spot the Difference



60

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 emails 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. ...

61

Types of Scams Review

Impersonation – make sure you are speaking to a legit company and not scammers posing as one.

Tech Support – Don’t allow remote access to anyone.

Online Shopping – Research merchants and look for red flags such as very low prices.

Payment – Be wary if you are asked to make a purchase with a promise of compensation.

Romance – Be leery of a relationship formed online with someone asking for money.

Financial – When your finances are concerned, you should always have space to make the best decisions for you and talk it over with those you trust with your money.

62

In Conclusion

While high pressure sales tactics are also used by legitimate business, it isn't a good idea to make important financial decisions quickly. Always take your time where your finances are concerned.

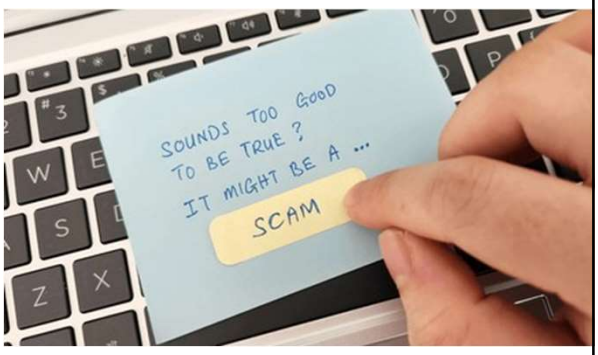
The best way to deal with a scammer is to **completely ignore them**. Scammers want things from others, and they want to steal things. If you ignore them, they don't get what they want, they will eventually give up.

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.

63

In Conclusion



64

CBBCBank

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.

Questions?

Beth Pyle
Branch Administrator, Senior Vice President
(865) 977-5906
bpyle@cbbcbank.com

Jonathan Settlemire
Chief Operations Officer, Senior Vice President
(865) 379-2506
jsettlemire@cbbcbank.com

65