INTERNET SAFETY
A Quick Review

Thea Martin
thea.martin@comcast.net
412-600-8640
THE BASICS

- General Internet Safety
- Facebook Safety & Privacy
- Get Rich Schemes
- Online Romance & Catfishing
MOST VULNERABLE TO INTERNET FRAUD
Bank Accounts
Amazon Accounts
Social Media Accounts
  • Facebook
  • Twitter
  • Instagram
BANK ACCOUNT INFO – SCAM!

Dear valued customer of TrustedBank,

We have received notice that you have recently attempted to withdraw the following amount from your checking account while in another country: $135.25.

If this information is not correct, someone unknown may have access to your account. As a safety measure, please visit our website via the link below to verify your personal information:

http://www.trustedbank.com/general/custverifyinfo.asp

Once you have done this, our fraud department will work to resolve this discrepancy. We are happy you have chosen us to do business with.

Thank you,
TrustedBank

Member FDIC © 2005 TrustedBank, Inc.
AMAZON REWARDS – SCAM!
SCAM! SCAM! SCAM!

Google Account Phishing Scam
SCAM!

We need your help

Dear Customers,

We need your help resolving an issue with your account. To give us time to work together on this, we've temporarily limited what you can do with your account until the issue is resolved.

We understand it may be frustrating not to have full access to your PayPal account. We want to work with you to get your account back to normal as quickly as possible.

What’s the problem?

We need a little bit more information about you to help confirm your identity.

Case ID Number: PP-001-487-260-335

Click To Confirm

How you can help

It’s usually pretty easy to take care of things like this. Most of the time, we just need a little more information about your account or latest transactions.

To help us with this and to find out what you can and can’t do with your...
What can I do?
CREATE STRONG PASSWORDS
AND CHANGE ON A REGULAR BASIS

- Baklava123
- Georgie2014
- Fluffy1
CONSIDER.....

- FMB!7daw – Feed Me Baklava! 7 days a week
- mgi4AHIP! – my georgie is 4 And He Is Precious!
- F8ambags? – Fluffy 8 all my baklava and got sick?
I WON! IT’S FREE! I’M GETTING MONEY!

- It’s not free
- You didn’t win
- No one in Nigeria has left you money — for a small fee....
If it’s too good to be true, it’s too good to be true!
YOUR PRINCE HASN’T COME...AT LEAST NOT FROM NIGERIA
YAY! I’M GETTING PAID TO SHOP ONLINE!

SCAM!

The online shopping fraud
They have their bank details stolen or are sent faulty items after buying something from an illegitimate online company.

The average amount that most people lose on a fake purchase: $300 USD

Tips:
1. Show them how to check the website link is genuine by hovering the mouse over it and making sure it matches the hyperlink.
2. Tell them to pay for items over $150 USD by credit card as they can claim the money back.
ONLINE ROMANCE & CATFISHING
ONLINE ROMANCE SCAMS

- Motivated by money
- Scammers are patient – will wait months to build a trusting relationship before asking for money, usually for an emergency or transportation, from the person they have conned into a relationship.
- They start off asking for small amounts of money and eventually build up to asking for larger amount of money or gifts.
- A victim believes in true love and believes that they have found it.
• Creates an online profile and makes contact with vulnerable victims using social media or dating apps.
  • Facebook
  • Match.com
  • Plenty of Fish
  • Farmersonlydating.com
  • Greekdates.com

• Develops a trusting relationship by isolating and grooming the victim, learning as much as possible about the victims family, background, dreams, and assets.

• Finds a way to get the targets money.
ANATOMY OF A ROMANCE SCAM

- Contacts victim
- Grooms victim
- The Sting
- The fraud continues
Declares their feelings early and pushes the relationship forward quickly

Has a profile with only a few photos and very few friends

Claims to have a job that means they have to travel all the time (often abroad)

May claim to be in the military, stationed abroad

Always has a last-minute excuse for why they can’t meet

Refuses to use a webcam or Skype

Tells you about a difficult situation and asks for money
CATFISHING

- In a typical catfish scheme, the catfisher sets out to deceive the victim, but does not at first intend to take money from the victim.
- The common denominator for victims is that they believe in true love, and they believe that they have found it.
- The BBB estimates that at any one time there may be 25,000 fraudsters online.
- Victims rarely speak out because they are humiliated and embarrassed because they have fallen for a scammer.
DECLARES THEIR FEELINGS WAY TO FAST AND IS PUSHING THE RELATIONSHIP FORWARD
HAS A PROFILE WITH FEW FRIENDS AND MIGHT BE A LITTLE TOO GOOD LOOKING
CLAIMS TO HAVE A JOB WHERE THEY TRAVEL ALL THE TIME – MIGHT BE IN THE MILITARY
REFUSES TO USE A WEBCAM OR SKYPE
NEVER WANT TO MEET
ASKS YOU FOR MONEY!
IF YOU THINK THAT YOU ARE A VICTIM

- Do not be embarrassed
- Call the police
QUICK OVERVIEW

- Everyone is vulnerable to internet fraud
- Change passwords regularly
- Don’t click on links unless you know 100% where the email has come from
- Do not under ANY circumstances send money to anyone who you do not know
THANK YOU!