Top Internet Scams

Overall Top Five Scams

In 2022, the Internet Crime Report (IC3) revealed:

- Total complaints received: 800,944
- Total Loss: $10.3 billion

Top Five Scams:

- Phishing/spoofing-300,497 complaints
- Personal Data Breach-58,859 complaints
- Non-payment/non-delivery-51,679 complaints
- Extortion-39,416 complaints
- Tech Support-32,538 complaints

Overall Top Five Scams

Phishing:

- The use of unsolicited email, text messages, and telephone calls purportedly from a legitimate company requesting person, financial, and/or login credentials.

Spoofing:

- Contact information is deliberately falsified to mislead and appear to be from a legitimate source.

Phishing/Spoofing Examples

- IRS requesting payment for back taxes by gift card. Threatening arrest for failure to pay.

- Job postings that request money and promise to send money back. Go to trusted websites to apply for jobs or go to the Career Center.

Example of Phishing

From: Customer Support [mailto:support@citibank.com]

Sent: Thursday, October 07, 2004 7:53 PM

To: Eilts

Subject: NOTE! Citibank account suspend in process

Dear Customer:

Recently there have been a large number of cyber attacks pointing our database servers. In order

to safeguard your account, we require you to sign on immediately. This personal check is requested of you as a precautionary measure and to ensure yourselves that everything is normal with your balance and personal information. This process is mandatory, and if you did not sign on within the nearest time your account may be subject to temporary suspension. Please make sure you have your **Citibank(R) debit card number and your User ID and Password at hand**. Please use our secure counter server to indicate that you have signed on, please click the link here. Note that we have no particular indications that your details have been compromised in any way. Thank you for your prompt attention to this matter and thank you for using Citibank(R)

Regards,

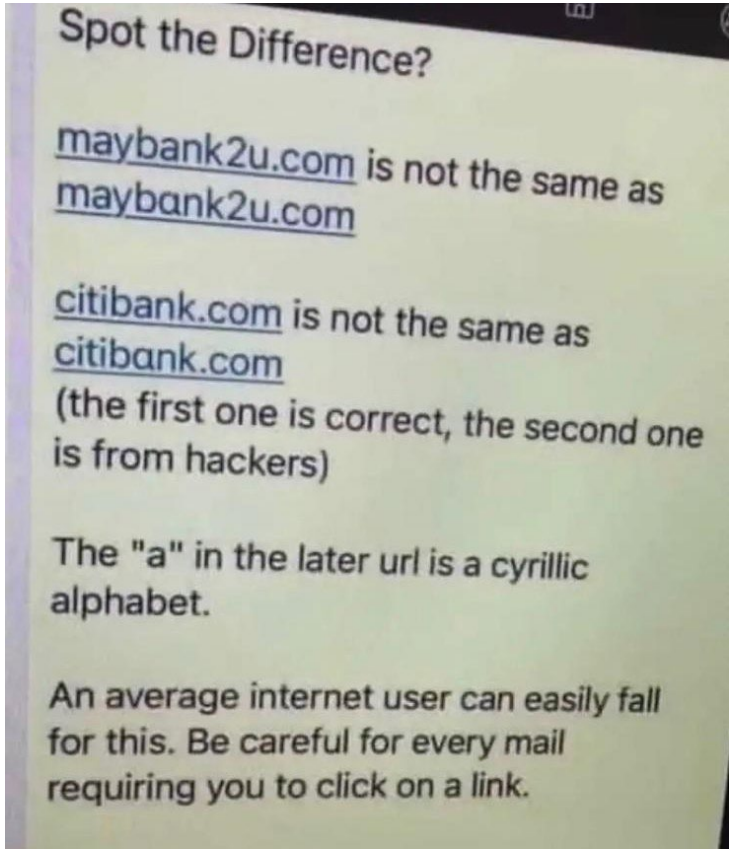
Citibank(R) Card Department

(C)2004 Citibank. Citibank, N.A., Citibank, F.S.B.,

Citibank (West), FSB. Member FDIC.Citibank and Arc

Do not click links in suspicious emails. Always go directly to the official website to ensure the legitimacy of information.

Phishing Example



Overall Top Five Scams

Personal Data Breach:

A leak/spill of personal data which is released from a secure location to an untrusted environment. Also, a security incident in which an individual's sensitive, protected, or confidential data is copied, transmitted, viewed, stolen, or used by an unauthorized individual.

Personal Data Breach Example

- Equifax data breach in 2017-the personal information of 147 million people was accessed by hackers. Names, addresses, dates of birth, social security numbers, drivers' license numbers, and credit card numbers were exposed.

Overall Top Five Scams

Non-Payment/Non-Delivery:

Goods or services are shipped, and payment is never rendered (nonpayment). Payment is sent, and goods or services are never received, or are of lesser quality (non-delivery).

Non-Payment/Non-Delivery Example

- Buyer pays for a good or service they find online, but those items are never received.
- Goods or services are shipped, but the seller is never paid.
- Auction fraud-a product is misrepresented on an auction site, such as eBay.
- Apartment rental postings that request money for what turn out to be fake leases. Go to Commuter Student Services & Off-Campus Living for assistance in finding housing.

Overall Top Five Scams

Extortion:

Unlawful extraction of money or property through intimidation or undue exercise of authority. It may include threats of physical harm, criminal prosecution, or public exposure.

Sextortion:

Suspect may threaten to release videos or pictures to your social media connections if you do not send money.

Do not exchange intimate photos or send personal information over social media or text message regardless if you know the person. This is a common scam affecting Stony Brook students and young adults.

Extortion/Sextortion Example

- Social media (Instagram, Facebook, etc.) - Suspect will contact the victim via social media and ask to take the conversation to another platform. Once there, they will ask to exchange nude photos or videos. After photos or videos are exchanged, they will threaten to release the photos to all their contacts if the victim does not send money.

Overall Top Five Scams

Tech Support:

Subject posing as technical or customer support/service.

Contact occurs through telephone, pop-up messages, locked screen on a device, or a combination of pop-up message and locked screen accompanied by a recorded, verbal message to contact a number for assistance. Once contact is made with the victim, the subject tries to convince the victim to provide remote access to their device.

Tech Support Scam Example

Emerging Scams

Business Email Compromise (BEC)- a scam targeting businesses or individuals working with suppliers and/or businesses regularly performing wire transfer payments.

Investment Scams- Deceptive practice that induces investors to make purchases based on false information. These scams usually offer victims large returns with minimal risk (Retirement, Ponzi, Pyramid). This is the costliest scheme reported to the IC3.

Crypto-Investment Scams- Investment scams involving crypto currency.

Ransomware- A type of malicious software designed to block access to a computer system until money is paid.

Government Impersonation- A government official is impersonated in an attempt to collect money.

How to Tell Something is a Scam

- Asks for personal information
- Promises that you can win money, make money, or borrow money easily
- Asks for payment via wire transfer or gift card
- IRS/ Government agencies will not request payment over the phone or by gift card
- Threatens you will be arrested if you do not send money
- Says family or friends are injured, arrested, or were in an accident and request money to help them

How to Tell Something is a Scam

- Uses scare tactics or pressure to act immediately
- Gives you a check or money order and asks to send some of the money somewhere
- Requests your bank account or credit card number when you are not making a purchase with that account
- Refuses to stop calling after you've asked not to be called again

What to Do If You Become a Victim

You should immediately take some basic steps to prevent additional crimes and begin repairing the damage.

1. Obtain a copy of your credit report and contact all three of the credit reporting agencies: Equifax, TransUnion, and Experian.

What to Do If You Become a Victim

2. Notify all credit card companies, creditors, banks, and financial institutions where you have accounts.

3. Consider putting a security freeze on your credit report. You can freeze your credit online for free at each credit agency.

What to Do If You Become a Victim

4. File a report with your local law enforcement agency.

5. Change all the passwords on your computer, making each one different.

6. If you believe you have been the victim of an internet scam, such as phishing, visit the Internet Crime Complaint Center at http://www.ic3.gov.

7. Contact the Federal Trade Commission to report fraud at: www.ftc.gov