Pegasus Protects- July: Account Take Over

In today's digital age, account security is more critical than ever. With the increasing sophistication of cyber threats, it's essential to stay vigilant and informed. One of the most concerning issues facing online users today is account take over – when unauthorized individuals gain access to your accounts, potentially compromising your personal and financial information.

How does it happen?

This type of criminal activity is achieved by obtaining the account holder's login in credentials through various types of attacks including phishing, malware attacks, social engineering, data breaches, and impersonation scams.

Some scenarios include:

If you receive an unsolicited text or email from your bank with a code for your online banking and you were not attempting to log in, report it to your bank immediately.

If you receive a code via text or email and someone calls to obtain that code, do not provide it. This is usually a tactic used by hackers.

How to protect yourself

- Monitor emails and other forms of communication:
- Set up multi-factor authentication. This is a method that requires the user to provide two or more verification factors to gain access to the log in. This is usually a form of an email or text with a code, a fingerprint validation or a security question.

- Don’t click on anything in an unsolicited email or text message asking you to update or verify account information. Look up the company’s phone number on your own (don’t use the one a potential scammer is providing), and call the company to ask if the request is legitimate.
- Change your password at least every quarter.
- Be careful what you download. Never open an email attachment from someone you don't know, and be wary of email attachments forwarded to you.
- Carefully examine the email address, URL, and spelling used in any correspondence. Scammers use slight differences to trick your eye and gain your trust.

You’ve been scammed, now what?

- Cease any activity on the computer, phone or device that has been suspected of being compromised. Disconnect the network connections and isolate the system. Engage with an IT professional to scan for and remove any malware.
- Contact your bank and request assistance with the access to your accounts. You can contact us at 214-353-3000.
- Try to obtain a written timeline of what has occurred, what has been lost and the steps take to report to financial institutions and credit agencies. Record the date, time, phone number and person who you spoke to.
- File a police report if there has been financial loss. Obtain the police report number, date, time, location and officer’s name regarding the report.

FAQs

How safe is online banking on my cell phone?

Mobile banking is considered safe if you use a secure internet connection and access your accounts from the trusted app. Add an extra layers of security by setting up multi-factor authentication and fingerprint or face ID.

What is the safest way to bank online?

The safest way to bank online is to access your bank’s official online or mobile banking app using a secured Wi-Fi connection or your phone’s mobile data. Banking with unverified or untrusted apps or over unsecured Wi-Fi connections could leave you vulnerable to cyberattacks. If you are in a public place it is recommended not to use the free Wi-Fi to log in to banking sites.

Scan the QR code to download our app

Below are some websites with additional information on account take over scams.

https://www.security.org/digital-safety/account-takeover-prevention/

https://www.forbes.com/advisor/banking/how-to-protect-your-online-banking-information/

https://www.mcafee.com/blogs/privacy-identity-protection/online-banking-simple-steps-to-protect-yourself-from-bank-fraud/

(edited 06/26/2024)