LPL Financial

Account Takeovers

What Account Takeovers Are and How to Defend Against Them

What is an Account Takeover?

Account takeovers occur when an unauthorized user gains access to an account. The severity of the takeover depends on a variety of factors, including what account they gained access to, what their intentions are, and how long they have access for. Bad actors typically attempt to gain access through a few different techniques, including social engineering tactics and technical exploits. Once an attacker has access, they can use the account in whatever manner they desire. Including potentially stealing more login information, payment information, or using the account for illegal activities.

The best way to defend against account takeovers is to ensure that you are using safe security practices and have a strong awareness for social engineering attempts. By educating yourself on what account takeovers are, and the methods and strategies attackers use to complete them, you will be better prepared in the event of an attack.

Most-Prevalent Attack Strategies

Bad actors use a multitude of different strategies to implement successful takeovers on victim's accounts. Understanding how attackers initiate these attacks is crucial in defending them.

Credential Stuffing: Often, bad actors have access to the dark web where data leaks can be found. There they can obtain millions of username and password combinations. If a bad actor successfully accesses one account, they'll often try the same login information on other websites or platforms, especially if the user reuses the same credential. Many times, this process is automated for threat actors and can allow them to gain access very quickly. That's why it's important for anyone affected by a data leak to change their password right away.

Phishing: Phishing is a form of cybercrime in which criminals deploy fraudulent communications to a user or organization that appear to come from a legitimate source. Bad actors have been increasingly creating more sophisticated phishing schemes with the help of AI to build elaborate, well formatted phishing campaigns. Within a phishing email is typically a malicious executable in the form of an attachment, link, or image.

Malvertising: Many times, cyber criminals will utilize online ad space to lure victims into being infected. By purchasing legitimate online advertising space, malicious actors can create the appearance of a trustworthy advertisement, while concealing harmful code embedded within it. In the case of account takeovers, the bad actor may install malicious code that copies cookie sessions and sends it to the bad actor. Resulting in a cookie theft or "session hijacking". If the bad actors can gain access to your computer's cookies, they may be able to load up a website's session and resume it as if they were the actual user. Thus, gaining access to the account and taking it over.

Man-in-the-Middle (MITM): MITM attacks occur when an attacker intercepts traffic on an unsecure network and hijacks a session. This is only possible if the attacker can intercept unencrypted traffic, usually only occurring in unprotected public Wi-Fi sessions such as an airport, amusement park, coffee shop etc. Bad attackers can interact with the session and pose as the authentic user without the real user ever being notified. Utilizing a VPN or using a hotspot instead of unprotected Wi-Fi is the best way to combat man-in-the-middle attacks.

Defensive Strategies:

Using a multi-layered approach to security is crucial for building a strong defense against threat actors and reducing the chances of becoming a victim of an attack.

Utilize Strong Passwords: Creating a long, complex password helps protect you from hackers being able to easily crack your password. In addition, you should use various passwords across accounts. This will prevent attacks from being successful at gaining access to multiple accounts if one of your accounts is compromised.

Use a Password Manager: Password managers are an application that can store and encrypt your passwords. They act as a vault that can safely store your passwords, allowing you to retrieve them when needing to access an account. They typically require longer, 15 characters passwords, as well as MFA before granting access to the stored password, making them more secure and difficult for bad actors to compromise. If a bad actor were to access the passwords stored within, the encryption would prevent them from being able to use the credentials to their purpose, as they would be unreadable.

Enable Multi-Factor Authentication: Enabling MFA on your accounts adds an extra level of protection as it requires a second form of verification, such as a code from your phone or email, or a biometric confirmation before granting access. This makes it more difficult for threat actors to access accounts and devices protected by MFA, because they would need access to the second device.

Report Phishing Emails: Bad actors continue to evolve their tactics of phishing campaigns. It's important to be aware of the warning signs. Be cautious towards external or unverified senders, avoid clicking unknown links or attachments, be aware of common scam tactics attackers may use.

Be Aware of Unusual Activity: Many times, even if you are not directly notified of an account takeover, there could be clues indicating that an attack is taking place. Regularly check credit statements, unusual account activity, or unauthorized communication not made on your behalf. If any of these things are taking place, then you may be affected by an account takeover and you need to take immediate actions to stop the attack.

What to Do if You Are a Victim of an Account Takeover

While understanding your enemy and applying effective strategies is crucial in mitigating your tactics of falling victim, it does not totally eliminate the possibility. If you are unfortunately affected by an account takeover, it's important to follow the steps below to prevent the attack from continuing.

Disconnect the Infected Device from the Internet. By disconnecting from the internet, you can safely perform tasks on your computer such as malware scans, antivirus and removal. Disconnecting from the internet will prevent the attack from escalating into something more harmful, like a ransomware attack. Be sure to work with your local IT professional to make remedial measures on your device to ensure there is no further compromise within your system.

Change your Passwords: If any of your accounts have been compromised by an attack or data breach, you should change all affected accounts immediately. You should also change the password to crucial accounts, including your password manager (if you utilize one), bank accounts, and your email passwords.

Freeze your Credit and Bank Accounts: If a bad actor gains access to your account, they may be able to use your credit or financial information for their purposes. Freezing your credit will prevent financial fraud from happening with your credentials. Not only should you prevent accounts from being created with your credentials, but you should protect your current bank accounts and freeze them while the incident is active. You can also reach out to your banking contact and inform them of the cyberattack to make them aware of and on the lookout for any fraudulent transactions on your account.

Takeaway

Ultimately, account takeovers are on the rise among bad actors, and their techniques of attacks will continue to become more sophisticated. But with the correct defensive strategies and good security practices, you can greatly reduce your chances of falling victim to an account takeover.