HOSTILE TAKEOVERS

Protect Yourself from Fraudsters Hijacking Your Accounts

Account takeovers occur when a criminal gets access to one of a victim's online accounts, changes the password (locking out the owner), and then proceeds to make large purchases, spend loyalty points like frequent flyer miles, steal personal information or impersonate the owner in other ways.

The takeover of one of your online accounts is a big problem you'll want to prevent. Account takeovers account for over $5 billion a year in theft and are growing faster than 50% a year. That's because bots can attempt 100 attacks per second using information from a half-trillion stolen documents on the dark web.

How fraudsters lock you out.

Crooks often begin by sending the victim a realistic-looking — but fake — email. The message is usually urgent, requiring immediate attention. The victim clicks on a link in the email, which automatically downloads bad software to their computer or phone.

…Or the victim clicks on a link and enters their username and password on a form, giving the crook access.

Crooks often gain access to an account for days…or even months…before taking it over.

Steps to take now, before trouble hits.

- Use a unique password for every online account, and make each password long and difficult to guess. This limits the damage if a crook gets access to one.
- Make a list of every online account you have, including your username or member name and password, plus contact phone numbers. Remember to include login information for your bank and mortgage company, financial accounts like PayPal, eBay and Venmo, social media accounts including Facebook and Twitter, e-commerce retailers where you shop including Amazon and Walmart, plus Apple (for iTunes), Microsoft and Google (for Gmail).
- Also note answers you've given to personal security questions some of the accounts require.
- Store this list in a secure place.
- Turn on "two-factor authentication," so a second password is sent to your phone via text or email to verify and permit each login.
- Use biometrics such as a face or fingerprint scan on your phone wherever possible.
- Review monthly financial statements from each of your accounts to ensure there's no suspicious activity.

If an account is taken over and you can no longer log in.

- Visit the help section of the company's website immediately and search for "account takeover."
- Don't create a new account until you're certain the existing account can't be recovered.
- Visit the Federal Trade Commission's *identitytheft.gov* website to learn more and build a recovery plan.

NTSC
NATIONAL TECHNOLOGY SECURITY COALITION