From the desk of
Michael Aliperti
MS-ISAC Chair

Compromised Email Account? Here's What to Do

An email account can be compromised in a number of different ways. In some cases, your password may be weak and easily guessed or obtained through a public breach. In other cases, you may have clicked on a malicious link in an email, social networking site, or webpage. Or, you may have downloaded an app or file that contained malicious scripts.

In this edition of the security newsletter, we'll look at potential warning signs that your email account may have been compromised, what you can do to recover, and steps you can take to help prevent it from happening again.

How to Tell if Your Email Account is Compromised

Here are some red flags that may indicate your account has been compromised:

1. **You are unable to access your e-mail account.** If an attacker gained access to your email address and password, they may have logged in and changed the password to lock you out of the account.
2. **Your family, friends, and coworkers receive emails from you that you didn't write.** Once your email account is compromised, the attacker can use your email address to send spam or phishing emails to the contacts in your address book.
3. **You see activity on your social media accounts that you didn't post.** Some social media sites use single sign-on (SSO) with credentials from other accounts (e.g. Google, Yahoo) so you can login to social media without having to create a separate username and password. If your email account is linked to your social media accounts or if you use the same username and password for all your accounts, the attacker can gain access to everything with a single username and password.
4. **You notice your Sent messages folder is empty or includes messages that you did not send.**

What to Do if Your Email Account is Compromised

Here are some steps you can take if your account has been compromised. If you think your account has been compromised but you are not sure, it is better to err on the side of caution and follow these steps:

1. **Login to your email account and reset your password using a strong password.**
   a. Use long passphrases to make passwords easier to remember and more secure.
   b. Do not use information about yourself, the city where you were born, your age, or the names of relatives, friends, or pets.
   c. Do not use common words such as the name of favorite sports team.
   d. If you are unable to login, contact your email provider to find out how you can regain access.

2. **End / sign out of all sessions on all devices.** Even after you change your password, if the attacker has an active session, they may be able to continue to send emails from your account.
3. **Reset any additional accounts that the attacker may have gained access to.** These may include financial institutions, shopping sites, and social media sites. There may be references to these accounts in your email. Remember to use unique passwords for each and every account. If not, if one account gets compromised, they all become compromised.
4. **Enable Multi-Factor Authentication (MFA) on your e-mail account.** This provides an additional layer of protection to login to your email account. It requires a code from a text message, phone call, or authenticator app to further verify access. Visit STOP.THINK.CONNECT to learn how to activate MFA.
5. **Review and change your security questions.** If your email account was compromised from a device or location not matching your normal usage, it's possible a malicious individual was able to answer your security questions.
6. **Review your mailbox for any rules that you have not previously created.** These rules can include message forwarding, deletion, or running unwanted applications.
7. **Review outgoing messages and retract any malicious outgoing messages.** In most cases, the attacker will not leave traces of any outgoing messages, but this should still be checked.
8. **Contact the people in your email address book and let them know that your email was compromised.** Remind them to delete any emails from you during the time your account was compromised to prevent them from becoming the next victim.
9. **Verify if there is private or personally identifiable information in your e-mail that could be used maliciously.**
10. **Establish a routine where you change your password periodically.** Consider changing your password on at least an annual basis (unless a breach requires it sooner).
11. **Scan your computer for viruses and malware.** This is especially important if you are experiencing problematic signs like unfamiliar applications loaded on your device, your computer operating slowly, or problems shutting down.

What Can I Do to Prevent an Email Account Compromise?

Good security best practices and safe browsing habits can help prevent your email account from being compromised in the future:

1. **Make sure your devices are patched with the latest updates, including antivirus.**
2. **Set your security software, internet browser, and operating system to update automatically.** Or, establish a routine to do this manually on a frequent basis.
3. **Use unique strong passwords for account access.**
4. **Be wary of unexpected emails, especially when they contain links and/or attachments.**
5. **Verify the sender's address.** If you don't recognize the address, don't reply.
6. **If an email request from a known contact seems out of place, verify the request by calling the sender on the phone.**
7. **Think twice before clicking a link.** Always hover before clicking to see the address of the web site you are attempting to visit.

8. **Never click text links like “Click Here” or “Unsubscribe,” or any other links in suspect emails.**
9. **Never input a password or your email address on an unknown site, and never provide your passwords to anyone.**
10. **Be vigilant when reviewing emails, as you may receive an email from a legitimate contact who has been compromised.**
11. **Don’t access your email account on a public computer or from a device using public Wi-Fi.**

Additional Information

- CISA: Choosing and Protecting Passwords
- CIS: Securing Login Credentials
- Stay Safe Online: Hacked Accounts
- FTC: Hacked Email