

How to Protect Your Email Account from Hackers

Have you ever received an email from a friend that they really did not send? Perhaps they were stranded in London with no money and needed you to send money?

Hackers love to get into your email account. Once they have access, they steal your contact list, and send scamming email to your friends, and sell their contact information on the black market.

Email hacking is very common these days. The cases I have seen involve sending fraudulent and virus laden emails to every person in the contact list. Most likely the hacker is also selling the contact list information to spammer clearinghouses. There are several ways this scenario can happen, including keystroke loggers, password crackers, and interception of unencrypted internet traffic.



Greg Miller

Here are some basic steps to take to prevent this from happening to you.

- First, you must have a strong password for your email account. This means using passwords that are totally random, and that use combinations of letters (upper and lower case), numbers, and special characters. The password **MUST** be eight or more characters, otherwise it is very easy for password cracking software to decipher.
- Using a password manager makes generating and using strong passwords simple. Plus, password managers go a long way in protecting you from keystroke loggers. LastPass is a highly regarded password manager and is free.
- If you don't want to use a password manager, then another good option is to use a long phrase. A phrase such as "Mary had a little lamb" is easy to remember, and has so many characters that it is difficult to crack.
- When using online email, be sure that your email browser uses https: (rather than http:); most do not. This ensures that your email ID/password are encrypted as they pass through the internet.
- When using your laptop at a Wi-Fi hotspot, ensure that your internet session is fully encrypted. This is usually not the case.
- Your computer should have antivirus and anti-spyware products that are up to date and functioning, and your PC should have all critical security patches installed. This minimizes the risk of getting malware that can steal your password as you type.
- If possible, avoid the free email services such as those from Hotmail, Yahoo, Excite, Gmail. These services are prime targets for hackers and often do not provide adequate security policies. It is much safer to set up a hosted email account with your own domain name. Having your own domain name costs only \$10 to \$20 per year, and a hosted email account can cost around \$2 per month.

These are the bare minimum steps that should be taken to provide basic protection.

Greg Miller is President of CMIT Solutions of Orange County, in Goshen, NY. He provides IT services to The Biondo Group, and serves as our company's Chief Information Officer in conjunction with our Cybersecurity efforts.

Excerpted from Biondo's Perspectives 3rd Q 2016