Hacked Email

On several occasions over the past few weeks I received an email from a customer whose content was obviously not from them. In one case, it simply contained a web link to a web site. In another case, there was a web link with the message "This is amazing – you have to check this out". Being ever vigilant, I of course did not click the links and immediately notified the sender that their email account had been hacked.

The situation described above is one of the more common ways to find out that your email account has been hacked. Another is that you begin to receive bounced emails from addresses you don't know. In the most severe case, you discover that you can no longer log into your account, either because the password has been changed or your account has been blocked by your email provider.

How Email Accounts Get Hacked

There are several ways that email accounts get hacked:

1) You have a weak, easily determined password. This is by far the most common mistake. It is made even worse if you use the same, easily guessed password on many sites.
2) You gave the hacker your password. You may say this could never happen to you, but there are many techniques where you believe you are communicating with a legitimate party (a friend or business), but actually are not. The communication might be via email, instant messaging, or on a web site. The obvious remedy is to never give out your password unless you are either creating a new account on a legitimate site, logging in to a legitimate site, or changing some account settings. No legitimate site will ever ask for your password in an email or any other form of general communications.
3) You stayed logged in on a public computer. Perhaps you were in a library, computer store, or internet café, and took the opportunity to check your email. This is never a great idea, but if you have to do it, be sure you log off before leaving the computer.

How to do if your Email Account is Hacked

First and foremost, time is of the essence. A hacked email account can be at best annoying and at worst devastating.

If you can log into your email account, and see that you have a large volume of bounced emails from strangers, then this is actually better news. It means that a professional spammer has gotten a hold of your email address and has used it in the reply-to field (a process called "spoofing"), but hasn't actually breached your email account. This is an important difference since having your account password compromised means your entire collection of email correspondence and email addresses have been exposed, whereas a spammer spoofing your address means the spammer doesn't actually control anything. Unfortunately, once a spammer starts using your email address, you really have no recourse but to close the account.

If your password no longer works for your email account and you are positive it is the correct password, then someone else has likely taken control. If you have lost control of both your email address and password and you use this combination on a variety of web sites including social network sites, financial sites, shopping sites, etc, then you are in big trouble (please make sure you don't have this exposure by using different strong passwords on each of your accounts.) If a spammer got into your email account and then sent out millions of spam emails, the account provider might have shut down your account and is waiting to hear from you to go through the process of authenticating you so that the account can be opened again.

Each account provider has its own method for determining that you are who you say you are. This might involve asking standard security questions, specific details about emails you have sent, or even the exact date you set up the account. All these steps are usually done on line, so before doing anything, you want to make sure your computer is current with OS updates, anti-virus/malware software, and free of viruses. Here is a list of common email providers that you can use to regain control of your email account:

- aol.com, aim.com
- att.net, sbcglobal.net
- btinternet.com, btopenworld.com, talk21.com
- comcast.net
- cox.net
- gmail.com, googlemail.com
- hotmail.com, msn.com, hotmail.co.uk
- inbox.com
- live.com, windowslive.com, live.ca
- mac.com, me.com
- mail.com
- myspace.com
- yahoo.com, rocketmail.com, ymail.com, yahoo.co.uk, yahoo.ca

If the emails sent by the spammer are for a personal appeal for money or help, or if malware was attached, then you should send an email to everyone in your contact list to ignore the content and to delete those messages immediately.

Set up at least two email addresses. Use your original as you normally do, but establish the secondary email address for communication with your account provider should you find yourself in this situation again. You might even set up a third email address as a "sacrificial lamb" and only use it for registering on web sites, newsletters, and other similar activities. Most importantly use a different and strong password for each account (see the article entitled "Strong Password Article" on my website for suggestions on how to create strong passwords.)

Once you have regained control of your email account and changed the password, check all your email settings. In particular, make sure a signature has not been added, that your email is not forwarded to another address, and that no automated filters have been installed that might do things like forward emails or attach files.

As always, I hope you have found this information useful. If you do not wish to receive these emails in the future, let me know.

This newsletter, as well as all past newsletters, can be found on my web site (http://steve.gimnicher.com).