What to Do if Your Email has Been Hacked

by Ross Hendry

On average each month I find at least 5 of my customers have sent me emails that automatically go into the 'Spam' folder of my email. The truth is that they did not send anything, either they or one of their contacts, have had their email or email contacts hacked, and it is the hackers who cause the spam emails to be sent.

Gmail filters my incoming email very efficiently, using all of the mail that passes through their systems, their servers have a massive record of spam emails, so to find these I have to go looking in my SPAM folder.

Mostly they are quite recognisable. The email that is addressed to me, looks like it has been sent by my customer but with bad grammar and spelling, a link with little or no explanation and usually a greeting and sign-off that your contact would never use.

I usually send an email to the contact warning them of some foul play with similar advice to this, but often they are aware of the problem and immediately think it is their email that has been hacked.

1. Change your password
If the hacker has accessed your account they have done so by "cracking" or " hacking" your password. Change it immediately, but totally. Do not change it from "ross123" to "ross1234", in fact you should steer clear of using any proper names in your passwords, contact me for a guide to creating a strong password you may use with every account!

2. Secure your Email account
In my experience most of these attacks simply send out an annoying email to your contacts, however, if you are unlucky they may change your password (preventing you from accessing your account), steal and delete your email contacts or even delete all of your email. If you are able to access your account, change your password immediately (see 1 above). If you are unable to access your email account you should be able to use the 'lost password procedure' to get back into your account. If this does not work you must contact your email provider and request their help in resetting your password.

3. Report the incident to the email site
Even if you were able to access your account you should report the incident to your mail service provider. They may be able to advise of further information on how you were hacked and how to prevent it in the future. They may have tools and backups to help reinstate your information if it has been deleted. It is crucial that you notify the service provider as soon as you know you have been hacked to increase the possibility of recovering any deleted data.

4. Announce the News
Now is the time to let your contacts know it was your email that was hacked and plead for their forgiveness! Most will have sussed out that you are not going to make them millionaires, or provide the best Viagra in the world and that you have been hacked. But just in case, warn them not to open any "funny or unsolicited emails" recently received from you.

5. Scan your computer with an updated anti-virus program.
Your PC may have been infected, by design, when you opened your mail account, so give your PC a thorough scan for viruses and malware.

Using your antivirus program, scan your full system and remove anything nasty found. If you do not find anything then I strongly recommend using Malwarebytes or Herd Protect and ensure that you remove/fix any items found.

If you do find something you must change your password again, because the nasty you found could have been relaying your newly changed password to the hackers!

6. Don't fail to review your personal email settings
Not only should you check your personal email settings, hackers often change these to enable them other possible ways of compromising your account. For example, they may change the setting that forwards every email you send or receive to another account (one of theirs) where your email is monitored for account details, passwords and other things associated with your identity and/or finances.

I have known hackers to turn on the auto-responder and send out spam messages to every incoming email! Another way they may do this is to modify your email template to send out a spam message at the end of each email you send like an email signature! It is at this time you should also review your security for this site. Normally you are asked some security questions that may be used to help if you lost your password, these now need to be changed as hackers have been known to record these for future use. Every little bit of this type of information may be used to help steal your Identity in the future.

7. Change passwords or security questions for other sites
Do you use the same login or password or combination of them for more than one account? Yes, that is right, the account or accounts with these must be changed too. This is why you are advised not to use the same Login data for more than one account.

8. Check your email folders
I know that I have sent people sensitive information from my email, such as bank account information titles and account numbers etc,. and other financial data such as my National Insurance Number. Some may still be in my email archive, did the hackers find this? The way to check is search your email for the word "password" or "account number" or "Login" then check the mail found, and delete it or secure it in another way. The best advice is to keep this type of email to a minimum and never send all information in one single email. If you do have to send bank details, send most by email but maybe text the account number by mobile telephone or even write a traditional letter - with a pen!!

9. Be on your guard
I do not mean patrol your PC, but be wary of your information. If heaven forbid the hackers found your National Insurance number it can be a major piece of information for them to find out more about you and so steal your ID. If you think or suspect that you have been hacked, then just be extra vigilant for the month or so after - check all of your financial accounts regularly, you may want to change the account login and passwords for them as well.

10. Prevention
We cannot stop sites our data resides upon being hacked, we cannot stop our family and friends' accounts being hacked, but we can create a strong password that makes cracking it virtually impossible. Avoid proper names as these are the most common hacked words. It is a known fact that people choose passwords based on readily available information, making their accounts 'crackable' with a few educated guesses. Easy passwords make it easier for hackers and spammers that use programs that can cycle through thousands of logins a second to identify weak accounts.

Ross Hendry is the proprietor of Interface Consulting and Engineering, who has over 42 years experience in Communications, Computer Technology and Direct Marketing. (See advert below).