Protecting and recovering from email hacking

Over the last 12 months I have received emails from more than 20 friends and acquaintances (mostly doctors) who didn't send those emails. More often than not I find the emails in my 'Spam' folder as Gmail knows they are not genuine. The subject lines of the emails are usually enough of give away that something is a bit fishy. Consultants who taught me many years ago, who I never really knew well, would not typically write "You have to check out this awesome website." These messages are the result of email hacking and raise several questions:

1. What is the best action to take if you receive such an email?
2. What is the purpose of the email hacking?
3. How can email hacking be prevented?
4. What should you do if your own email account is hacked?

What is the best action to take if you receive such an email?

It's not a great idea to open the emails if you know from the outset that they are from a compromised email account. Although it's rare, the mere act of opening an email to read it can trigger a malicious payload. There isn't much of a risk if you use Gmail, Yahoo or similar. It's more of a problem if you use a PC based email program (like Outlook or similar). Certainly don't click on any links in 'fishy' emails. All sorts of bad things can start trying to get into your computer (or smartphone).

Don't reply to the email or send an email to the sender. It may seem like a good idea to reply but email is not the way to do it. The best response is to contact that person via another means. Send them a text, a Facebook message, call them or maybe an email to a different email address. Let them know you suspect their email account has been hacked (or compromised) and that it looks like it's sending out emails to people in their address book.

What they should do in this situation is Google 'what to do if my email is hacked' or read the instructions laid out at the end of this article.

The final thing you should do is delete the email (just in case it contains something nasty).

What is the purpose of email hacking?

In this context, the purpose of the hacking is usually to spread these unsolicited emails to everyone in the target's address book. These are usually advertising emails or (more likely) designed to infect recipient computers or smartphones with malware. This is usually achieved by text in the email that encourages the recipients to visit a particular website. The websites may be able to lever weaknesses in the recipient's computer or smartphone to inject malware. Such malware can result in a wide variety of consequences too numerous to describe here.

How can email hacking be prevented?

The main target email accounts are the common web-based email services, like your personal Gmail, Yahoo, Hotmail or Outlook.com accounts. These are the main targets for a number of reasons. Firstly, web email accounts can be accessed (or hacked) from anywhere in the world. Secondly, personal accounts usually will receive all the password reset emails. That's relevant because if a hacker also wants access to your Amazon account they can just choose 'I've forgotten my password' on Amazon.co.uk and use the password reset email to gain control. The third reason your personal, web-based, email is at most risk is because millions of people use the same system, so bulk attacks can result in a lot of reward for the hackers. On the other hand, your work email accounts are much less of a target. Often they have extra layers of security to access emails, especially out of the UK. In addition, they generally wouldn't be used as password reset accounts. Finally, far fewer people are on one work system, so there is less gain from a single attack. Work or corporate accounts are still attacked but not usually by this common unsolicited email approach.

There are a few steps to protect your personal email accounts:

- Ensure your computers aren't already compromised. Check you are running up-to-date anti-virus / malware software (not as necessary on a Mac).
- Ensure your email password meets the following criteria (if not, change it so it does)
  - Unique (don't use it on any other website)
  - Absolute minimum of eight characters long, complex, ideally including punctuation (the longer, the better).
- For even better security add 'Two Factor Authentication' (covered in a previous issue).
- Consider using a password manager to help remember your new password (Lastpass covered in a previous issue).
- Remember not to reuse your new, more secure, password on any other sites.

As a final point of interest, I wouldn't generally recommend frequently changing your password. If you have a high quality, unique, password there is no need to regularly change it. It doesn't become less secure with age. The reason work and corporate environments force their employees to change their passwords frequently is to reduce the risks of password sharing. Hopefully most of you wouldn't share your personal email password or your Amazon password, as they are valuable. The same is often not the same for work login details. Staff share them with colleagues frequently, and these passwords are then more likely to fall into the wrong hands. Forcing frequent password changes limits the utility of sharing your work password with a colleague.

What should you do if your own email account is hacked?

If you become aware your email account has been compromised your first step is to ensure you can access your account. If you can, change your password as above. If you can't, try the password recovery options that your email company provide. They will often include sending a password reset link to a secondary email address or via text. Once you have access to your account check your inbox or deleted emails for password reset emails from other websites (in case the hackers have tried to gain control of other accounts). Next, check you still have access to your other important accounts like Facebook, Apple, Amazon, etc. If you have used the same (or a similar) password on another site, change the password on those sites to unique strong ones too. Lastly, check your sent email folder. If you can see people who may have received unsolicited emails from your account, you should let them know too (ideally not by email).

Mr David Haider,
Consultant Ophthalmologist and Chief Clinical Information Officer, Bolton Foundation Trust, UK.
E: david@drhaider.co.uk
Twitter: @drdavidhaider