What Do I Do When My Email Has Been Hacked and Spam Is Sent to My Contacts?

Your computer was most likely compromised in one of four ways. 1) You do not have up-to-date security software installed. 2) Your passwords are weak and easily hacked. 3) You clicked on a malicious link in an email, IM conversation, or on a social networking site, or webpage.4) You downloaded a game, video, song, or attachment.

When your email account is hacked, here are several steps you need to take:

1. **Check your computer's security.** Most hackers collect passwords using malware that has been installed on your computer (or mobile phone if you have a smartphone). No matter which operating system you use, be sure your anti-virus and anti-malware programs are up to date. Choose the setting that will automatically update your computer when new security fixes are available. If you cannot afford security software, choose one of the free security suites available. To find these, type 'best free security software reviews' into your search engine.

Look to see that all operating system updates are also installed. To find these, type '(the name of your operating system) and updates' into your search engine. Set your computer to update automatically so that you get protection from new attacks as soon as possible.

2. **Change your password and make it stronger.** Do this after your anti-virus and anti-malware programs are updated or the hackers may collect your new password as well.

    - Strong passwords do not have to be hard to remember, they just have to be hard to guess.
    - Make your password at least 10 characters long, and use capital letters, lower case letters, numbers and symbols.
    - Do not use information about yourself or someone close to you (including your dog or cat!) like name, age, or city.
    - Do not use words that can be found in a dictionary, these are easy for hackers to break, even if you spell them backwards.
    - Text messaging shortcuts can help make strong memorable password creation easier. For example L8rL8rNot2Day! translates to later, later, not today.

3. **Send an email to your contacts saying you were hacked.** When an email comes from someone you know you are more likely to open it and click on links within it – even if the subject is weird. Help stop the spread of the malware by warning those in your contact list to be cautious of any email sent by you that doesn't seem right, and to not click on the links.

4. **Smarten up about Spam phishing, and scams.** Spam comes at us from all angles; in the mailbox in front of your home (junk mail) in your email inbox, via IM, social networking sites, chats, forums, websites, and sadly, now also on your phone.

    - You do not have a rich uncle you've never heard of in some foreign country trying to send you money. You have not won the lottery. No stranger is going to give you money for any reason. No hot babe is lonely and waiting for your response. The only things you'll get via an unsolicited pharmacy offer is ripped off or an infection (on your computer or phone). If there really was a miracle weight loss cure, it would be front page news and on every TV station.

    - No reputable bank or company is ever going to ask you to 'authenticate' information online. And if you get an email with a link to one of these sites, don't use it; instead, use your search engine to find the site yourself, and then log in. If the message was legitimate, the message will be waiting for you in your account.

5. **Validate the legitimacy of any program/game/app/video/song before downloading it.** According to a study released in June 2011 by Microsoft, 1 out of every 14 programs downloaded by users is later shown to be malware, or having malware attached to it. If content is pirated, free, or comes to you anonymously, assume it has malware. Only download content that you have read good reviews about from sites you can trust.

If you are a Hotmail user, there is a feature that can help you, or others you know who have had their email account hijacked. Called "my friend's been hacked" and found under the "Mark as" dropdown, a simple click allows friends to report compromised accounts directly to Hotmail.

When you click that button, a report is sent to Hotmail where that report is combined with other information to determine if the account in question was in fact hijacked.

Once the account has marked as compromised, two steps are taken:

- The account can no longer be used by the spammer

- You (or your compromised friend) are put through an account recovery flow that helps you take back control of your account.

If you are a Hotmail user but your hacked friend uses a different email service, the alert will be sent to their email provider. For example, the alert could be sent to Yahoo! or Gmail so these companies can take action.

http://protectme.webroot.com/internet-safety-tips/beginners-tips-getting-started-in-internet-security/what-do-i-do-when-my-email-has-been-hacked-and-spam-is-sent-to-my-contacts.html