Safeguard your email account from hackers

Author : Cat

Date : October 8, 2014

At least once a month I get a strange email from one of my contacts. Sometimes it is a link which is masked as a funny article I must look at. Sometimes it is a plea to send $1000 immediately to Costa Rica because they are stranded there with their family. How and why does this happen?

There are two ways this is typically done; An email that *appears* to be from the sender in which case the hacker has a copy of their contact list. Or, an email from the sender's account that they did not send, in which case the hacker has actually gained access to the account. Safeguarding against these situations is easy. Let's discuss both.

Appearances can be deceiving - stolen contact list

When you receive an email in your Inbox, you are usually greeted by the sender's name. Depending on the software or device you use to read the message, the sender's email address may also be visible. Hackers rely on you not checking the email address, just the name. If they can get a hold of your contact list, they can send emails to all of your contacts using your name as the display name. When people you know receive it, they will open it and read the contents as if you sent them. The example pictured above shows just this. Though I have blocked out the name, this message appeared to have been sent from someone I know with the title "This is the sweetest thing I have ever seen"; however, the email address associated with it is for a site called W!nkal, not my friend. Clicking on the links in this email could have done any number of things to me from acknowledging that the email address is valid to planting a virus on my computer.

Has it happened to you? Since the messages are not being sent from your account, there is no way to tell if this has happened from your end. Typically, one or more of your friends will message you to question the email or let you know they received it.

How to fix it: Regrettably, once a hacker has your contact list, you cannot get it back. What you can do is email your contacts to let them know that someone has done this and that the emails are not from you. This will pre-emt the damage done if they were to click on the links.

How to prevent it: To get into your address book, you need to grant an application permission to do so. If you receive an email from another hacked victim and click on the link, you may be allowing some foreign application to access your contacts. If you receive an email that seems short or not personal that has a link, hover over that link with your mouse to see where it is going. If you don't know the website, don't visit.

Many social networks will ask if you want to find your friends. This allows that network to copy your address book with all associated email address in order to match other users. In most cases, the network will not give this information away, but if they do not have terms that indicates this, then you are at their mercy not to sell that information.

- **Do not click on strange links from emails**
- **Check for email addresses that match sender names in suspicious emails**
- **Do not grant access to your address book unless you trust the source**

That's mine and you can't use it! - stolen credentials

The only way someone can have full access to your account is to have your password. If someone is targeting you specifically, then they can try to guess your password. If they have access to your computer then they can get it if you remain signed in. If you are part of a system hack, for example a breach of Adobe's passwords, then an automated application takes all of the emails and passwords it has stolen and tries those same passwords against the corresponding email account.

Once a hacker is in your account they can use it to change your password and then you lose access. If ever you find your password is no longer working then you need to contact your email provider immediately to regain control.

Has it happened to you? Other than being locked out of your account, it is extremely difficult to tell if someone is using your account. If they do email your contacts then someone will hopefully tell you. If the hacker is particularly sinister, they may just be using your account to look for valuable information.

If you use the same password from your email in other places and are worried that your email may have been hacked in one of the major data breaches that occurred, you can use the site Have I Been Pwned?. This is a safe website. You enter in your email address and it will tell you if it appears on any of the lists it has from breached systems. You are not required to enter in any passwords.

How to fix it: Change your password. If you have been hacked by a person or system that has not locked you out then changing your password will prevent them from doing it again. If the hacker has made a copy of your contact list, there is nothing you can do to get it back. As above, email your contacts to let them know that someone has done this and that the emails are not from you. This will potentially pre-emt the damage done.

How to prevent it: Since account access is all about your password, keep it safe.

- **Use different passwords for all accounts, especially email**
- **Do not use a guessable password**
- **Do not stay signed in at a computer that others can access**

Protect your contact list, protect your password, and protect yourself.