Article: Hijacking Email - Phishing for information

Hijacking Email - Phishing for information | Tech Tips Article by PcCG

I received an email from my cousin with a bizarre looking link. No other information, no subject, no personal endorsement, just a link. This is certainly a hijacked account.

In today's world we have better spam filters and anti-virus software, however the endless cat-and-mouse game never ends. Instead of sending spam from random addresses, people often attempt to hijack accounts in order to send spam, or viruses.

If you receive a message from joe1232393@plitz.ru, odds are you will (or should) delete it right away. Do not pass go, do not collect 200 dollars. However if the message comes from my friend Jeff I may open and even click on the message. This is why hijacking accounts is becoming a big problem today. The spammers use this method to get past the spam filters and anti-virus software.

This "hijacking" is actually a result of "phishing" (pronounced fishing). Phishing is an attempt to trick someone into providing the phisher with sensitive information, namely your email account and password. It's the computer-equivalent to people trying to steal identities over phone-based scams.

In a phone based scam, you may receive a call from someone claiming to be from Visa. They may sound quite professional and convincing. This is in order to make you feel comfortable giving out your information. They will tell you that your account has had some fraudulent activity and that they need to verify your account information. They will then ask you to provide your credit card number, full name, and 3 digit number on the back. And you will tell them "nope, ain't gonna happen!".

How do you deal with this? Inform the person you will call Visa back on the number listed on the credit card, and then confirm any information they may need. This way you know exactly who you are talking to (i.e. you know it is TRULY Visa.)

It's pretty much the same with computer phishing or hijacking. You visit a page that says you must log in to view content. You are then taken to a page that looks very much like yahoo's mail. You are made to feel confident you are indeed logging into yahoo. However if you look closely in the address-bar, you will see anomalies. The website may for example be "yah00.com" with zero's instead of "o's". Or it may say http://www.password-checker.com/yahoo. Cue buzzer-sound! Wrong answer again. It must say www.yahoo.com – then anything after that is fine. That must appear in the beginning of the address bar, not later on in the address bar such as password-checker.com/yahoo.com.

If you are tricked into entering your account information somewhere besides your actual email site, you've just given the bad guys your username and password. But the fight isn't over yet.
To date, MOST of the time when you are a victim of phishing/hijacking, a large amount of emails will be sent from your account. You will be notified by one of your friends most likely, that you are a victim of hijacking… well actually they'll probably say you have a virus which is inaccurate but I digress. You may also notice a lot of "failed to deliver" messages suddenly in your inbox, this is another sign you have been hijacked.

Fortunately the solution is usually simple. Change your password. That's it. Problem solved. The hijackers no longer have access to your email. Also check your security questions and alternate email addresses (if that option is present) to make sure they haven't been modified by the hijackers – so that they can't regain access to your email.

At this point you are probably good to go. However just to be safe, download malwarebytes at www.malwarebytes.org and install the free malware tool. Update it, and do a full scan on your system. It will certainly find things, but the chances are small it was related to the hijack. Also use a good anti-virus.

So to recap.. be careful where you enter your email address and password. If you do become a victim of phishing (hijacking), simply change your password, check your security questions in your email options then download and scan with malwarebytes.

I'd also send out an email to everyone explaining you were a victim of hijacking and to disregard any message sent from you that day. Then give them a link to this article! :)



Article Tags: Tech Tips [1]
Tech Tips Articles [2]
Email [3]
Hijacked [4]
Hijacking [5]
Phishing [6]
Spam [7]

Source URL:https://www.pccomputerguy.com/Email-Hijacking-Phishing-for-data

Links
[1] https://www.pccomputerguy.com/Tagged-Items-Under-Tech-Tips [2]
https://www.pccomputerguy.com/Tagged-Items-Under-Tech-Tips-Articles [3]
https://www.pccomputerguy.com/taxonomy/term/44 [4]
https://www.pccomputerguy.com/taxonomy/term/47 [5]
https://www.pccomputerguy.com/taxonomy/term/45 [6]
https://www.pccomputerguy.com/taxonomy/term/43 [7]
https://www.pccomputerguy.com/taxonomy/term/46