Email Hacked? 7 Things You Need to do NOW

Ask Leo! by Leo Notenboom

Helping people with computers... one answer at a time.

Ask Leo! » Email » Email Security

> Email account theft is rampant. If it happens to you there are several steps you need to take not only to recover your account but prevent it from being easily hacked again.

by Leo A. Notenboom, © 2012

It seems not a day goes by where I don't get a question from someone that boils down to their email account having been hacked.

Someone, somewhere, has gained access to their account and has started using it to send spam. Sometimes passwords are changed, sometimes not. Sometimes traces are left, sometimes not. Sometimes the everything in the account is erased, both contacts and saved email, and sometimes not.

But the one thing that all these events share is that suddenly several people, usually those on your contact list, start getting email from "you" that you didn't send at all.

Your email account has been hacked.

Here's what you need to do next...

1. Recover Your Account

Login to your email account via your providers website.

If you can, consider yourself very lucky, and proceed to step 2 right away.

If you can't login even though you know you're using the correct password, then it's likely that the hacker has already changed your password.

Use the "I forgot my password" or other account recovery options offered by your email service. This typically involves sending password reset instructions to an alternate email address that you do have access to, or perhaps answering the "secret questions" that you set up when you created the account.

If the recovery methods don't work - perhaps because the hacker

Is it on my PC or not?

Most people when faced with this situation immediately believe that some form of malware has entered their computer and is responsible for email being sent out from their

has also altered all the recovery information that might be used (changed the alternate email address or answers to the secret questions), or perhaps because you don't recall the answers, didn't maintain the alternate account or didn't set up any recovery information in the first place, then you may be out of luck.

If recovery options don't work - for whatever reason - your only recourse is to use the customer service options provided by that email service. For free email accounts there are usually **no** phone numbers or email addresses - your options are usually limited to self-service recovery forms, knowledge base articles and official discussion forums where service representatives may, or may not, participate. For paid accounts there are typically additional customer service options that are more likely to be able to help.

Important: If you cannot recover access to your account then it is now someone else's account. It is now the hackers account. Unless you've backed up, everything in it is gone forever and you can skip the next two items. You'll need to set up a new account, from scratch.

2. Change Your Password

One you regain access to your account, or if you never lost it, you should immediately change your password.

As always, make sure that it's a good password: easy to remember, difficult to guess, and long. The longer the better in fact, but make sure your new password is at least 10 characters or more, and ideally 12 or more if the service supports it.

But don't stop here. Changing your password is not enough.

3. Change Your Recovery Information

While the hacker had access to your account they may elect to leave your password alone. That way chances are you won't notice that the account has been hacked for a while longer.

But whether they changed you password or not, they may very well have gone in and changed the recovery information.

The reason is simple: when you finally do get around to changing your password the hacker can follow

account.

That is not the case.

In the vast majority of these situations your computer was never involved.

The problem is not on your PC. The problem is simply that someone else knows your account password, and is logging into your account online.

They could very well be on the other side of the planet from you and your PC (and often are).

Yes, it's possible that a key-logger on your PC was used to sniff your password. Yes, it's possible that your PC was used in a non-secure way at an open WiFi hotspots. So, yes, absolutely, scan it for malware and use it safely, but don't for a moment think that once you're malware free you've resolved the problem. **You have not.**

You need to follow the steps outlined to the right to regain access to your online account and protect your online account from further compromise.

You'll use your PC, but your PC is not the problem.

the "I forgot my password" steps and reset the password out from underneath you using the recovery information that he collected or set.

Thus, you need to check all of it, and change much of it ... and right away.

Change the answers to your secret questions. The answers you choose don't have to match the questions (you might say your mother's maiden name is "Microsoft", for example) - all that matters is that the answers you give should you ever need to recover your account match the answers you set here.

Check your alternate email address or addresses associated with your account, and remove any that you don't recognize or are no longer accessible to you. The hacker could have added his own. Make sure that all alternate email addresses are accounts that belong to you and that you have access to.

Check any mobile or other phone numbers associated with the account. The hacker could have set their own. Remove any that you don't recognize and make sure that if a phone number is provided it's yours and no one else's.

These are the major items, but some email services have additional information that they can use for account recovery. Take the time now to research what that information might be, and if it's something that could have been altered while the hacker had access to your account.

Overlooking information that could be used for account recovery could allow the hacker to easily hack back in - make sure you take the time to carefully check and reset as appropriate.

4. Check Related Accounts

This is perhaps the scariest, and the most time consuming.

Fortunately it's not common, but the risks are high so understanding this is important.

While the hacker has access to your account they have access to your email, including both what is in your account now - past email - as well as what arrives in the future.

Let's say that the hacker sees you have a notification email from your Facebook account. The hacker now knows you have a Facebook account, and what email address you use for it. The hacker can then go to Facebook, enter your email address and then request a password reset.

A password reset that's sent to your email account ... that the hacker has access to.

As a result the hacker, by virtue of hacking your email account, can now hack your Facebook account.

In fact, the hacker can now gain access to any account you have for which this hacked email is the email address of record.

Like, perhaps your bank. Or Paypal.

Let me say that again: because the hacker has access to your email account he can request a password reset be sent to it from any other account for which you use this email address. In doing so the hacker can hack and gain access to those accounts.

What you need to do: check your other accounts for password resets that you did not initiate, and any other suspicious activity.

If there's any doubt consider also proactively changing the passwords on those accounts as well. (There's a strong argument also for checking or changing the recovery information for these accounts just as you checked for your email account, for all the same reasons.)

5. Let Your Contacts Know

Some may disagree with me, but I recommend letting your contacts know that your account was hacked. Either from the account once you've recovered it, or from your new email account.

In particular, inform all the contacts in the address book that's kept with that account online. That's the address book that the hacker would have had access to.

I believe it's important to notify your contacts so that they know not to pay attention to email sent while the account was hacked. Occasionally hackers will actually try to impersonate you to extort money from your contacts. The sooner you let them know that the account was hacked, the sooner they'll know any such request - or even the more traditional spam that might have come from your account - is bogus.

6. Start Backing Up

One of the common reactions to my recommending you let your contacts know is: "But my contacts are gone! The hacker erased them all, and all my email as well!"

Yes. That happens sometimes. It's often part of a hacker not wanting to leave a trail - they delete everything in the account: everything they've done along with everything you've done.

If you're like most people you've not been backing up your online email. All I can suggest at this point is to see if your email service will restore it for you. In general they will not. Since the deletion was not their doing, but rather the doing of someone logged into the account, they may simply claim it's your responsibility.

Hard as it is to hear, they're right.

Start backing up your email now. Start backing up your contacts now.

For email that can be anything from setting up a PC to periodically download the email via POP3 or IMAP, to setting up an automatic forward of all incoming email to a different email account if your

provider supports that. For contacts it could be setting up a remote contact utility (relatively rare, I'm afraid) to also mirror your contacts on your PC, or periodically exporting your contacts and downloading them that way.

7. Learn From the Experience

Aside from "I should have been backing up" one of the most important lessons to learn from the experience is to consider all the ways that your account could have been hacked, and then taking appropriate steps to protect yourself from a repeat occurrence in the future.

- Use long passwords that can't be guessed, and don't share them with anyone.
- Don't fall for email phishing attempts. If they ask for your password they are bogus. Don't share your password with anyone.
- Don't click on links in email that are not 100% certain of. Many phishing attempts lead you to to bogus sites that ask you to login and then steal your password when you try.
- If you're using WiFi hotspots learn to use them safely.
- Keep the operating system and other software on your machine up-to-date and run up-to-date anti-malware tools.
- Learn to use the internet safely.
- Consider multi-factor authentication where simply knowing the password is not enough to gain access. Most services do not support this, but for those that do (Gmail, for example) it's worth considering.

If you are fortunate enough to be able to identify exactly how your password was compromised (it's not common) then absolutely take measures so that it never happens again.

8. If You're Not Sure, Get Help

If the seven steps above seem too daunting or confusing then definitely get help. Find someone who can help you get out of the situation by working through the steps above.

While you're at it, find someone who can help you set up a more secure system for your email, and can advise you on the steps you need to take to prevent this from happening again.

And then follow those steps.

The reality is that you and I are ultimately responsible for our own security. That means taking the time

to learn, and taking the time to set things up securely.

Yes, additional security can be seen as an inconvenience. In my opinion dealing with a hacked email account is significantly more inconvenient, and occasionally downright dangerous. It's worth the trouble to do things right.

If that's still too much ... well ... expect your account to get hacked again.

Article C5415 - June 1, 2012

Leo A. Notenboom has been playing with computers since he was required to take a programming class in 1976. An 18 year career as a programmer at Microsoft soon followed. After "retiring" in 2001, Leo started Ask Leo! in 2003 as a place for answers to common computer and technical questions. More about Leo.

You may also be interested in:

- Is changing my password enough? Changing your password is a common response to security breaches. Unfortunately, it may not be enough to recover.
- How do I use an open WiFi hotspot safely? Open WiFi hotspots at coffee shops, airports and other public places are opportunities for hackers to steal information. I'll review how to stay safe.
- Internet Safety: How do I keep my computer safe on the internet? Internet Safety is difficult. yet critical. Here are the seven key steps to internet safety - steps to keep your computer safe on the internet.
- What Security Software do you recommend? I have recommendations for specific products in various places on the site. Here's a short single page summary.
- Is this "Account updates!!!!!" email legitimate? "Account updates!!!!!" is a recent and frequent attempt at phishing. I'll break down why it's so obviously bogus, to show things to look for elsewhere.
- Is Windows Live Hotmail about to close my account? People continue to fall for what more experienced users would say are laughably bogus phishing attempts. I'll analyze why one common attempt is so bad.

http://ask-leo.com/email_hacked_7_things_you_need_to_do_now.html