HAS YOUR EMAIL ACCOUNT BEEN HACKED?

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

But the one thing all of these events share is that suddenly, 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

Log in to your email account via your provider's website.

If you can log in successfully, consider yourself *extremely* lucky and proceed to the next step right away.

If you can't log in, even though you *know* you're using the right password, then the hacker has probably changed your password. *The password you know is no longer the correct password.*

You must then use the "I forgot my password" or other account recovery options offered by the ISP (Internet service provider).

This usually means the service will send password-reset instructions to an alternate email address that you do have access to, or send a text message to a mobile phone number that you set up previously.

If the recovery methods don't work because the hacker changed everything, or because you no longer have access to the old alternate email or phone 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 phone numbers or email addresses provided by that email service. For free email accounts, there usually is *no* customer service. Your options are generally 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, *it is now someone else's account*. It is now the hacker's 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 and start over.

Is it my computer or not?

When faced with this situation, many people worry that malware on their computer is responsible. That is *rarely* the case. In the vast majority of these situations, your computer was never involved.

The problem is not on your computer. The problem is simply that someone else knows your password and has logged into your account. They could be on the other side of the world, far from you and your computer (and often, they are).

It's possible that a key-logger was used to capture your password. It's possible that your PC was used improperly at an open WiFi hotspot. So, scan it for malware and use it safely, but don't think for a moment that once you're malware free, you've resolved the problem. You have not.

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

2. Change your password

Once you regain access to your account (or if you never lost it), *immediately* change your password.

As always, make sure that it's a good password: easy to remember, difficult to guess, and long. In fact, the longer the better, but make sure your new password is at least 10 characters or more – 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 a hacker has access to your account, they might leave your password alone so that you won't notice the hack for a while longer.

But whether they change your password or not, they may change *all of the recovery information.*

The reason is simple: when you finally do change your password, the hacker can follow the "I forgot my password" steps and *reset the password out from underneath you,* using the recovery information they set.

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

- **Change the answers** to your secret questions. They don't have to match the questions (you might say your mother's maiden name is "Microsoft"); all that matters is that the answers you give during a future account recovery match the answers you set now.
- **Check the alternate email address**(es) associated with your account and remove any you don't recognize or are no longer accessible to you. The hacker could have added his own. Make sure all alternate email addresses are accounts that belong to you, and you can access them.
- **Check any phone numbers** associated with the account. The hacker could have set his own. Remove any you don't recognize, and make sure that if a phone number is provided, it's yours and no one else's, and that you have access to it.

These are the major items, but some email services have additional information they use for account recovery. Take the time *now* to research what that information might be. If it's something a hacker could have altered, change it to something else appropriate for you.

Overlooking information used for account recovery allows the hacker to easily hack back in; make sure you take the time to carefully check and reset all as appropriate.

4. Check related accounts

This is perhaps the scariest and most time consuming aspect of account recovery.

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

While the hacker has access to your account, he has access to your email, including what is in your account now as well as what arrives in the future.

Like your bank. Or Paypal.

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 you did not initiate, and any other suspicious activity.

If there's *any* doubt, consider proactively changing the passwords on those accounts as well. (There's a strong argument 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

Let your contacts know that your account was hacked, either from the account once you've recovered it, or from your new email account.

Inform all the contacts in the online account's address book; that's the address book the hacker had access to.

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

6. Start backing up

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 downloading the email, to setting up an automatic forward of all incoming email to a different account, if your provider supports that. For contacts, it could be periodically exporting your contacts and downloading them to a location on your hard drive.

7. Consider multi-factor authentication (in which simply knowing the password is not enough to gain access). More and more services are starting to support this, and for those that do (Gmail, for example), it's worth considering.