

## **Dealing with a hacked e-mail account**

Unfortunately, this is becoming increasingly common. These messages arrive via e-mail or you may encounter them on social networking sites.

To send out these messages, scammers hijack someone's account. They then send messages to the people listed in the person's address book. There are various ways to get into someone's account. But you likely fell for a phishing attack.

There is one very important thing to do in a situation like this. **You should call the person who owns the account—immediately.** It will eliminate any questions about the message's legitimacy.

The person may not even know that his account was compromised. The scammers may be collecting his confidential information. You should, of course, contact him via telephone. Otherwise, the scammers— maybe Nigerian, not Russian—can intercept your e-mail

Of course, he will want to go through his address book. He should notify everyone on the

list about the scam. Otherwise, they could become victims. I also recommend that you forward [this tip about recovering from a hacked e-mail account](#). He should just follow my steps.

Finally, you and he should report the scam. This is easier said than done. But, there's one great place to report online crimes. [Learn more about it here](#).

## **So your e-mail was hacked. Now what?**

A compromised e-mail account doesn't mean that your other accounts have been compromised but I would assume the worst and take immediate action.

The person who hacked your account is probably in another country. That's where most scams like this originate. So, you have to wonder how the hacker got your log-in information.

The hacker doesn't know you so he probably didn't guess your password. For the same reason, your password probably wasn't reset.

You could have been tricked by a phishing e-mail. Or, in a worst-case scenario, you have a keylogger on your machine. Keyloggers record your keystrokes. Some even take screen shots.

A keylogger wouldn't limit itself to e-mail passwords. It would record everything you do on the machine. It could capture credit card numbers, banking passwords and other log-in information.

**Get to work fast.** Start by securing your machine. You need one firewall and one antivirus program. You also need at least two anti-spyware programs. Get all of this for [free from my site](#)

Once you have the software installed, update it. You need to have the latest malware definitions. Then, run the programs one by one. They should detect and remove malware on your machine. I wouldn't be surprised if you find a keylogger.

You should also run Windows Update. This installs security patches for Windows and other

Microsoft software. Keeping software updated is just as important as running security software.

Flaws in other software can also open your machine to hackers. So run Secunia's Software Inspector. It will check for updates for other installed programs.

[My tip](#) covers everything you need to know about Software Inspector.

Securing your computer is only the beginning. Now you need to protect all of your online accounts.

You should change your password at every site you've visited on that machine. I recommend making a list of the sites you use. Go through your bookmarks and Web history, if need be. This will help you cover all bases.

When you create new passwords, [make sure they're strong](#). What's a strong password? My tip explains all. You'll probably also want a password manager. It will help you remember all of your passwords

I recommend the free KeePass program. You can download it from my site. But first, make sure you know how to use it. My tip provides [step-by-step instructions](#). **LOOK THIS UP ONLINE at komando.com**

There is a chance that you could fall victim to identity theft. So, you need to take some steps to protect yourself. I recently wrote a handy column on [protecting your identity](#). Read it and follow the steps. You'll be glad you did.

Now, all of this assumes that a keylogger is on your machine. But, maybe you remember entering your e-mail password on a suspicious site.

Should you go through all these steps if you fell victim to a phishing attack? You betcha! Many phishing sites install malicious software—especially keyloggers.

Besides, think about the information that could be in your e-mail account. There could be plenty of sensitive data. It's best to play it safe.