

You've Got (hacked) Mail!

Has your email account ever been hacked? Most people only hear of sensationalized cases of hacking, such as a celebrity or politician whose email was compromised, quite obviously, because of their high-profile status. Yet it can happen to anyone, and the reasons are quite varied.

At first, you may not even realize you've been hacked, but the following are typical signs of the problem:

- You can't access your account using your password.
- Someone tells you they've received odd messages from you via email.
- Your email account's activity (messages sent, received and stored) is gone.
- You don't recognize the messages in your "sent" folder.
- You receive a message from your own email address.

The reasons someone would hack an email account might include:

- **To send messages to your contacts as if they are coming from you.** The hacker may be trying to trick them into believing that you are in trouble and need their assistance, usually financial help.
- **To send other types of spam email.** The sender may get paid per click on a link within the email or may be trying to scam the recipient out of information, i.e. credit card details.
- **To gain access to your other accounts.** This is especially harmful if you've used the same password on the other accounts as you used on your email account.

Similarly, there are various ways the hacker may have accessed your email account:

- Your password is weak.
- You inadvertently downloaded malicious software, a.k.a. "malware."
- You lack security software or your security software is outdated.

If your email account is hacked, you need the following information to know how to respond:

- **Regain control of your account.** It may be as easy as resetting your password, but it may require contacting the online help center of your email service provider.
- **Use a new, hard-to-guess password.** Don't use this password on any of your other online accounts.
- **Change all security questions and answers.** This will help reduce the chance the hacker may be successful in subsequent attempts to access your email account.
- **Consider sending an email message to those in your contacts list.** Inform them your account was hacked and to be wary of recent messages sent from your email address.
- **Check for alternate email addresses.** These may have been added to your account for account recovery purposes. Delete any that may have been added by the hacker.
- **Add an alternate email address.** Add one of your own if you haven't already done so.
- **Run your security software.** This will help determine if the hacker downloaded any viruses/malware.
- **Check your other online accounts.** Be sure to check those connected to the hacked email address for signs of tampering. This is a good time to change those passwords and security questions/answers as well.

IMPORTANT NOTE: If you feel the hacking of your email account may have caused exposure of any of your personally identifiable information, always seek consultation with a Kroll Investigator.