

What to do if your e-mail is hacked

Standard steps to do if you believe your e-mail has been hacked:

<http://blogs.msdn.com/b/securitytipstalk/archive/2010/07/07/hotmail-hacked-take-these-steps.aspx>

While Hotmail is the most common target for hacking in the media, the instructions and general advice are good:

Courtesy of MSDN:

1. Change your password. (On the Windows Live Hotmail Web site sign-in page, click Forgot your password?)
2. Update and change the secret question and answer used to recover your password.
3. Update and change the alternative email address that you use on your account.

If you no longer have access to your account, please contact the appropriate administrator to restore access to your account.

- For Hotmail, try: <https://windowslivehelp.com/PasswordReset.aspx>
- For SSC e-mail, contact: <http://computing.sscnet.ucla.edu/public/contact/>
- For UCLA e-mail, contact: <http://www.bol.ucla.edu/>
- For Gmail (google mail), try:
<https://www.google.com/accounts/recovery?continue=http%3A%2F%2Fmail.google.com%2Fmail>

Additionally, we strongly recommend that you consider whether or not personally identifiable information has been compromised and contact your banks/credit cards/etc. for fraud alerts if they are at risk.

Courtesy of MSDN:

- Your credit card company, if you have given your credit card information. The sooner an organization knows your account may have been compromised, the easier it will be for them to help protect you.
- The Federal Trade Commission (In the United States). Report the circumstances to the FTC: National Resource for Identity Theft. <http://www.consumer.gov/idtheft/>
- The Anti-Phishing Working Group at spam@uce.gov.

Revision #1

Created Thu, Aug 19, 2010 6:15 PM by Won, Brian J.

Updated Thu, Aug 19, 2010 6:15 PM by Won, Brian J.