DAWSON COLLEGE

Information Systems and Technology
helpdesk@dawsoncollege.qc.ca
(514) 931-8731 xHELP (4357)

I got phished (or ransomed)!

This document explains what happens when your account gets hacked due to phishing or ransomware, and what corrective steps you should take.

How did my account get hacked?

Your account may have been hacked because you responded to a phishing email, most probably by tricking you to enter your credentials to a fake login page. For more information read our articles about phishing and actual examples. It is also possible you were victim to ransomware by opening a shared file from an infected colleague.

Why was my account disabled? Why can't I use Webmail?

Often the first thing hackers do with your credentials is to change your password and use your email account to spam other users. So you might unknowingly infect your colleagues, who are particularly at risk since they might trust an email seemingly coming from you.

When we detect this behavior **we automatically disable your account.** You must call Helpdesk to have it reinstated.

We also subject your account to a **stronger security group**. Accounts in this security group need their password changed every three months rather than yearly, and cannot access Webmail. Note that you can still get email on your mobile device, and at home through Outlook/Office 365 Pro.

What else is potentially compromised?

With your credentials, hackers had information to your files on the network drives, SharePoint, and information on MyDawson such as your courses and your pay stubs.

Your computer may have been infected with malware. This malware may not have visible effects to you: it can be *spyware* to track your Internet activity, *trojan* to use your computer as part of a network to launch denial of service attacks, *keyloggers* to record everything you type and therefore steal other sensitive information or passwords, etc. The malware may also be *dormant* and designed to launch under certain conditions or at a certain date.

Your personal accounts could now be target to hackers, especially if you have used your Dawson email in registering to third-party services, or provided it as a 'backup'. Obviously you are even more at risk if you have used a similar password to your Dawson password.

Some reputable corporations such as Microsoft and Google may be blocking your email because it was used for phishing.

What should I do next?

If you have a personal computer at home, run an anti-virus scan.

Change all your passwords, even your personal accounts. Make sure to use distinct passwords. Reusing the same 'seed' is not safe, e.g. 'XVB_lkv1' and 'XVB_lkv2'. For more information, see our article on choosing a good password.

If you have evidence that, even a few days after your account was reinstated, the emails you send are not getting through the recipients, call the Helpdesk.

Your best protection is knowledge and vigilance. You can start with this article with a few pointers.

How do I move out of the security group to get Webmail back?

If you wish to go back to the general policy (change password every year and access to Webmail), do the following:

- Go to the IST article on phishing. You may access this article from Dawson web site by searching for 'phishing'
- Read the article, and follow the link to the first quiz
- Take the quiz, more than once if necessary, to get a result of 80% or more
- Email a screenshot of your results to helpdesk@dawsoncollege.qc.ca
- Allow 24 hours for the changes to take effect