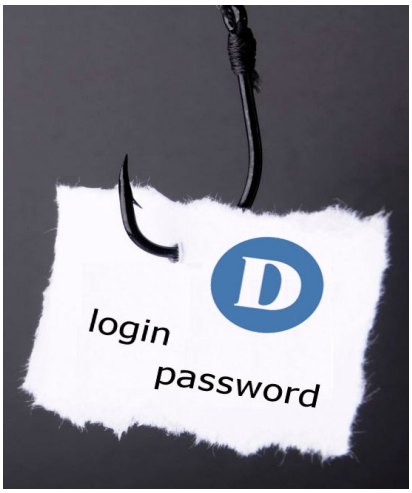
Information Systems and Technology

Beware of phishing scams

Phishing emails are fraudulent emails designed to look like legit emails, their purpose is to invite you to reply or follow hyperlinks to steal your personal information.



Our spam filters can intercept most phishing emails, but scammers can always find new ways.
Never respond or follow a link from a suspicious email!

If you have received such an email, please click: Report Phishing

Watch out for MFA scams

Some scams are designed to defeat Multi-Factor Authentication (MFA) by tricking you to sign in and enter your verification code on a fake, lookalike page. The scammers then immediately use this information to log into the real site as you. Another technique consists of asking for this information via a text message.

Never answer an MFA challenge you have not triggered yourself and never send a code or password via SMS.

This is what a legitimate email should look like

- ☑ Received in Inbox, not the *Junk* folder
- ☑ Sender's name matches their email
- ☑ Recipients are visible
- ☑ Gives instructions rather than a direct login link
- ☑ Signed with a name and the organization's contact

From: François Paradis <fparadis@dawsoncollege.qc.ca>
Sent: Friday, October 10, 2025 8:01 AM
To: John Smith
Subject: Your password is expiring soon

Your Dawson network password will expire in 5 days. To change it from a Dawson Windows workstation, press CTRL-ALT-DEL and select Change a password. From any browser, go to MyDawson and select Network account.

François Paradis
Information Systems and Technology
t (514) 931-8731 x1363 | www.dawsoncollege.qc.ca

More info and examples at : https://www.dawsoncollege.qc.ca/information-systems-and-technology/articles/phishing/.

Think you fell for it? Contact IT Support at x 4357.