February 22, 2018
Camrose Public Library

Online Safety 3: Spam, Scams & Pop-Ups

Scam vs. Spam

Scam: A fraudulent and often illegal business scheme

Spam: Unwanted and annoying emails; often-called junk. Many *scams* are orchestrated through *spam* emails.

Common Email Scams

1. Phishing
2. Nigerian 419 Scam
3. Lottery Scam
4. Guaranteed loan or credit card
5. Disaster relief scam
6. Travel scam
7. "Make money fast" chain email

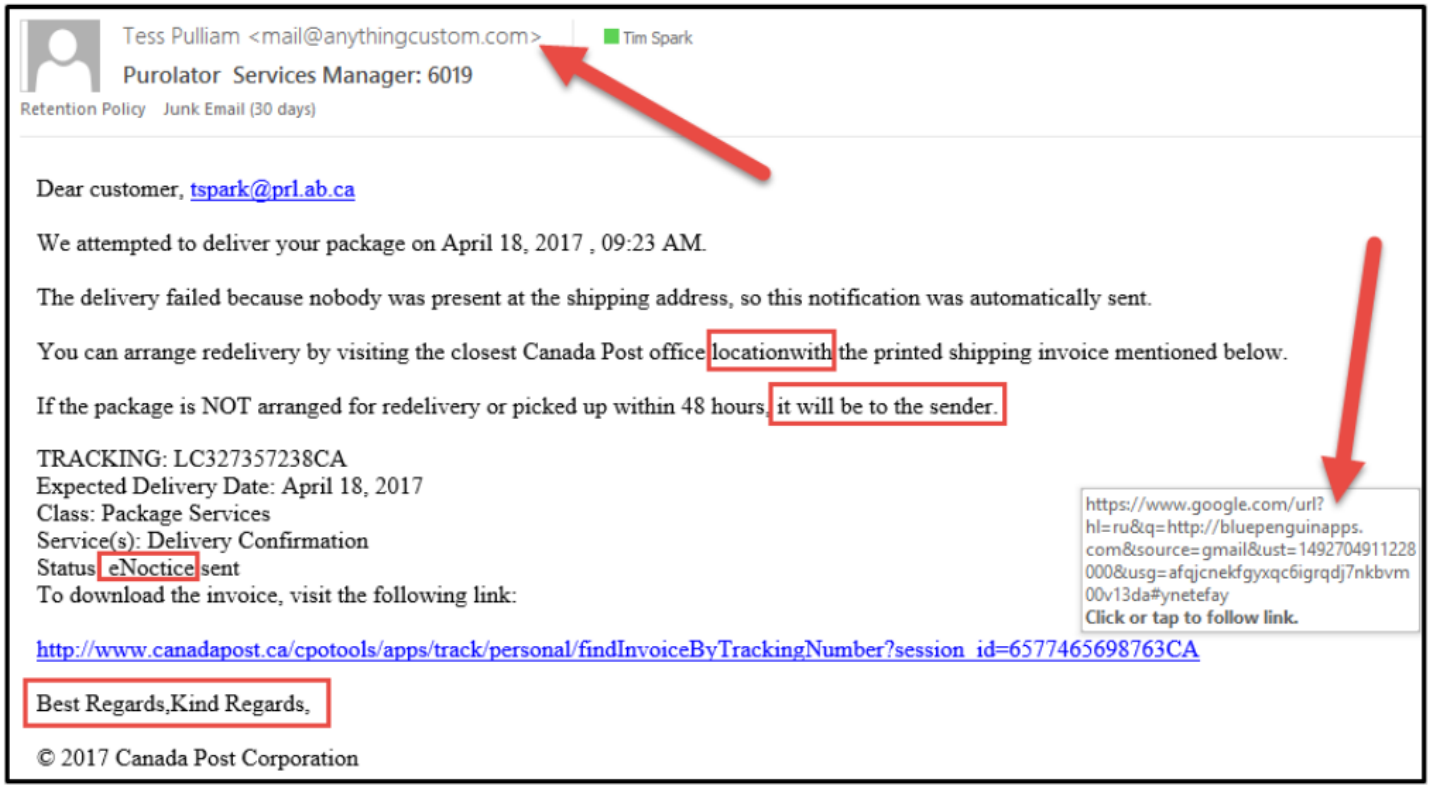
Email and Spam

- If you didn't request it, get rid of it!
- Is the email too good to be true? Remember, nothing is free!
- Look out for spelling mistakes, bad grammar, strange links and the sender's email address
- Never open attachments or follow links from a suspicious email
- If in doubt, call the sender. Don't respond to the email
- Add the suspicious email to your spam/junk folder

How to Mark Email as Spam

- Depending on what email provider you use, you can mark emails as spam so they don't show in your inbox
- You can easily look up the steps for marking spam by using the Internet
    - Using Google or another search engine, search for **"email provider (ex/ Telus, Outlook etc.) how to mark email as spam"**
    - You may need to see if there are different steps for different devices (ex/ iPad vs. Android tablet)

February 22, 2018
Camrose Public Library



Tess Pulliam <mail@anythingcustom.com>
Tim Spark
Purolator Services Manager: 6019
Retention Policy Junk Email (30 days)

Dear customer, tspark@prl.ab.ca

We attempted to deliver your package on April 18, 2017 , 09:23 AM.

The delivery failed because nobody was present at the shipping address, so this notification was automatically sent.

You can arrange redelivery by visiting the closest Canada Post office locationwith the printed shipping invoice mentioned below.

If the package is NOT arranged for redelivery or picked up within 48 hours, it will be to the sender.

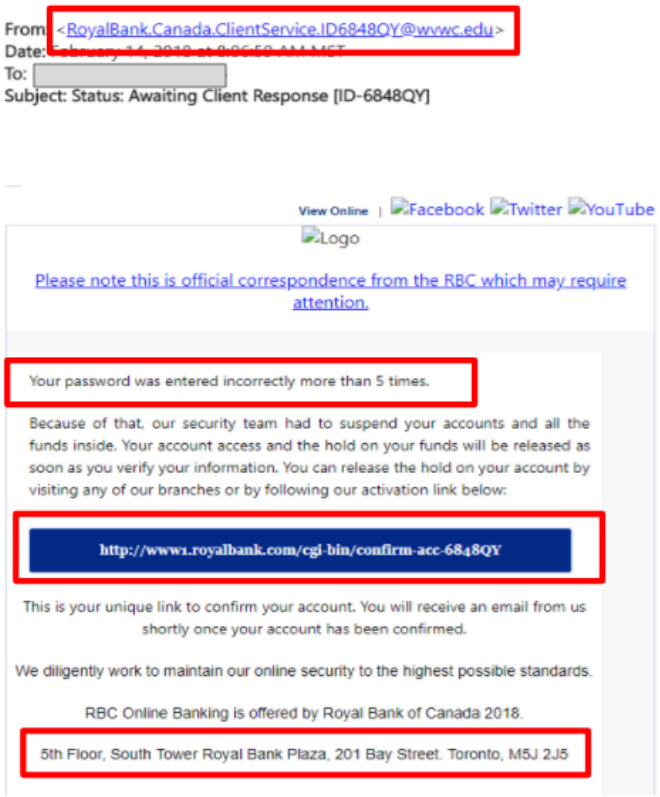
TRACKING: LC327357238CA
Expected Delivery Date: April 18, 2017
Class: Package Services
Service(s): Delivery Confirmation
Status eNoctice sent
To download the invoice, visit the following link:

https://www.google.com/url?hl=ru&q=http://bluepenguinapps.com&source=gmail&ust=1492704911228000&usg=afqjcnekfgyxqc6igrqdj7nkbvm00v13da#ynetefay
Click or tap to follow link.

http://www.canadapost.ca/cpotools/apps/track/personal/findInvoiceByTrackingNumber?session_id=6577465698763CA

Best Regards,Kind Regards,

© 2017 Canada Post Corporation



From: <RoyalBank.Canada.ClientService.ID6848QY@wvwc.edu>
Date: [redacted]
To: [redacted]
Subject: Status: Awaiting Client Response [ID-6848QY]

View Online | Facebook Twitter YouTube

Logo

Please note this is official correspondence from the RBC which may require attention.

Your password was entered incorrectly more than 5 times.

Because of that, our security team had to suspend your accounts and all the funds inside. Your account access and the hold on your funds will be released as soon as you verify your information. You can release the hold on your account by visiting any of our branches or by following our activation link below:

http://www1.royalbank.com/cgi-bin/confirm-acc-6848QY

This is your unique link to confirm your account. You will receive an email from us shortly once your account has been confirmed.

We diligently work to maintain our online security to the highest possible standards.

RBC Online Banking is offered by Royal Bank of Canada 2018.

5th Floor, South Tower Royal Bank Plaza, 201 Bay Street. Toronto, M5J 2J5

The sender email address does not look legitimate.

Designed to scare you into acting fast.

Close, but not the same address as RBC headquarters.

“Http” = Not secure
Never follow the link provided in the email. Legitimate institutions will not ask you to follow a provided link.

February 22, 2018
Camrose Public Library

Common Scams

Personal Emergency Scam

A message that appears to be from someone you know saying they are in distress. Find another way to verify if it is true, such as reaching out directly to the person.

You Owe Money Scam

If you hear from a bill collector or a government agency about money "owed" by you or a family member, don't respond unless you are certain it's legitimate. Contact the agency directly.

Online Dating Scam

Use a reliable and well-known dating website. When you meet someone online, watch out for red flags:

- If someone claims to be very young or wealthy
- If they use a picture that looks like it came from an advertisement
- If they pressure you to leave the dating site and want you to communicate by text or email
- If they profess instant feelings of love
- If they are never able to meet you face-to-face
- If they ask you to send money

Facebook Messenger Scam

If someone who is your friend on Facebook sends you a link or video, asking if it is you in the video, this is a scam. Do not open the message or follow the link. The message is often malware or steals your Facebook login information, automatically sending the same hoax message to your list of friends.

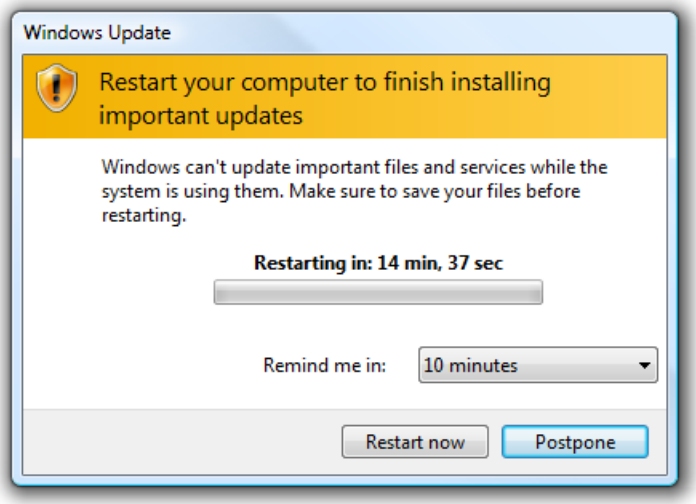
If you do open the message, you need to secure your account.

- Let your friends know not to open anything sent by you
- Reset your password
- Do an antivirus scan on your device and any needed updates

February 22, 2018
Camrose Public Library

Infected Computer Scam

- Keep your device up to date!
- If you are unsure if an update is legitimate, call the organization
- Or, take a picture and ask someone
- If a popup window is flashing, uses panic-inducing language or loud audio, don't click on it
- Turn off your device and talk to a tech expert



What To Do If You Are Hacked

- Turn off your device
- Report it
  - Contact local police and file a report
  - Notify the Canadian Anti-Fraud Centre
  - Contact your bank and credit card company
  - Contact the national credit bureaus and place a fraud alert on your credit report
- Reset Passwords
- Update your device and do a security scan
- Let friends and family know