

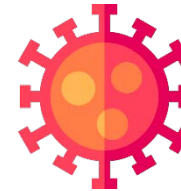
2020 Member Engagement Tour - Cybersecurity



Why is Cyber Security Important?



- The largest insider attack cost Boeing \$2 Billion and persisted for 30 years
- Yahoo holds the record for the largest data breach of all time with 3 Billion compromised accounts
- Data breaches exposed 4.1 billion records in the first 6 months of 2019
- Malicious attacks rose 600% since COVID-19 began
- 24% of data breaches are caused by human error



CRA Canada

Lessons Learned



- Disclosed that over 11 000 confirmed CRA accounts were compromised.
- This is one of the most impactful breaches in Canada's history as hackers attempted to change user details and siphon CERB payments.

What Happened?

- Malicious hackers used a technique called "credential stuffing" in order to compromise user accounts.

Credential stuffing is when malicious attackers find databases of already compromised usernames and passwords and then attempt to login with these credentials.

In laymen's terms, if someone is using the same username and password for both Facebook and the CRA, and if Facebook gets hacked, attackers can use those credentials to login to the CRA.

Passwords

- Do not keep passwords in plain text
- Do not keep passwords on paper

Length > Complexity

- DuckFerrari\$ will take 2 centuries to crack
- d9F%@fLq will take 5 days to crack

Amount of Time to Crack Passwords	
"abcdefg" 7 characters	🕒 .29 milliseconds
"abcdefgh" 8 characters	🕒 5 hours
"abcdefghi" 9 characters	📅 5 days
"abcdefghij" 10 characters	📅 4 months
"abcdefghijk" 11 characters	📅 1 decade
"abcdefghijkl" 12 characters	📅 2 centuries
BetterBuys	

- Use a Password Manager!
 - Local password manager
 - Keepass



- Cloud password manager
 - LastPass

LastPass...

Marriot Data Breach

Lessons Learned



- Disclosed that over 5.2 **Million** guest records were stolen.
- This is their second by Marriott in recent years following a breach in 2018.

What Happened?

- Malicious hackers used a technique called “spear phishing” in order to trick targeted employees into giving the hackers their Marriot domain accounts.

Spear Phishing is when malicious attackers target specific employees in order to trick them into either clicking a malicious link or attachment. Once they click the virus will infect their computer and compromise their system or network.

In laymen`s terms, an attacker did their research and sent a specially crafter email to 2 Marriot employees asking them to open up a malicious file



CPA

CHARTERED
PROFESSIONAL
ACCOUNTANTS
BRITISH COLUMBIA

Don't take the bait

How to stop and avoid
phishing emails



What is Phishing?

Any type of attempt to trick you into doing something to benefit the crooks.

- Opening an attachment in email
- Clicking on a link
- Sharing confidential information
- Transferring funds
- Credential theft



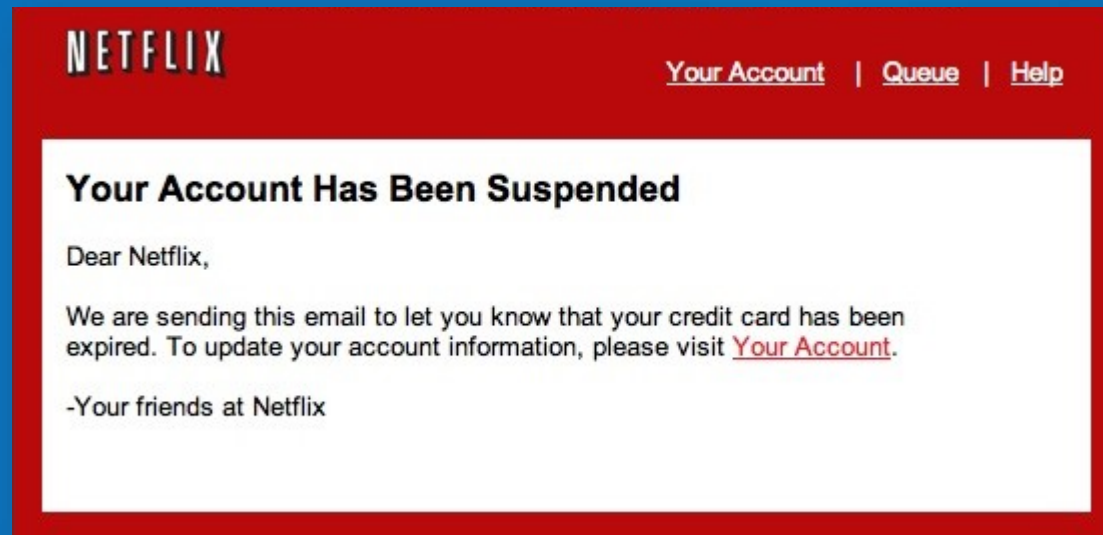
MASS
PHISHING



SPEAR
PHISHING

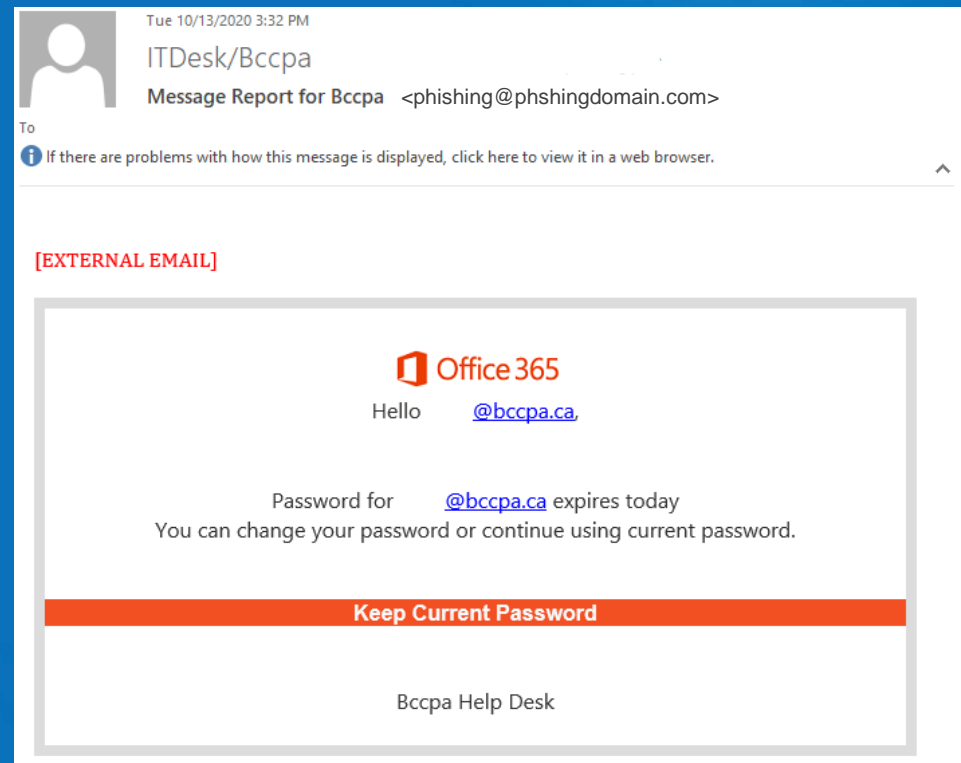
Mass Phishing

- **Target: Individuals' Assets**
e.g. bank accounts, identity, login credentials.
- Typically aimed at consumers
- Impersonal: mass email mail outs
- Credentials used or sold for financial gain



Spear Phishing

- **Target: The assets of a specific organization** e.g. data, money
- Typically target an individual or specific group in an organization
- Often use spoofed (look-a-like) email addresses
- Impersonate trusted sources and senior executives





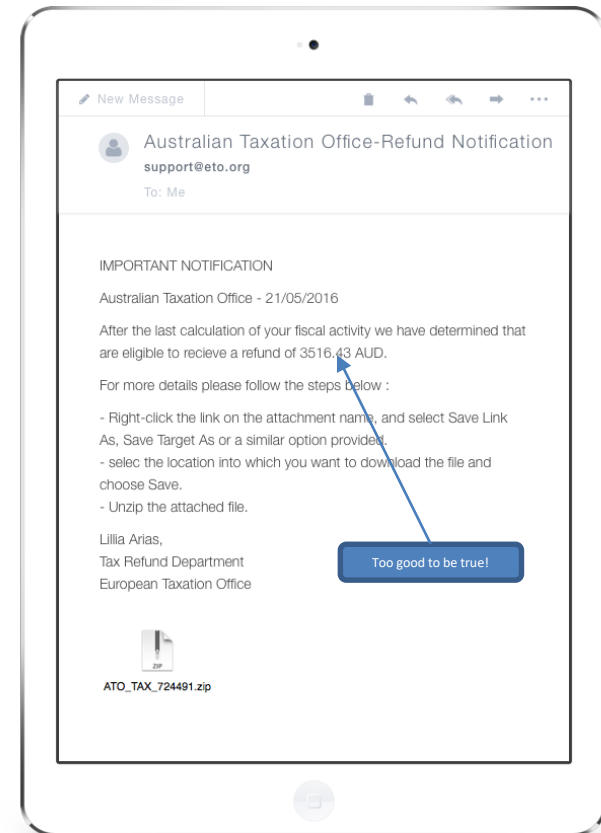
CPA

CHARTERED
PROFESSIONAL
ACCOUNTANTS
BRITISH COLUMBIA

Ten Tell Tale Tips To Spot Phishing Emails

Ten Tell-Tale Signs of Phishing

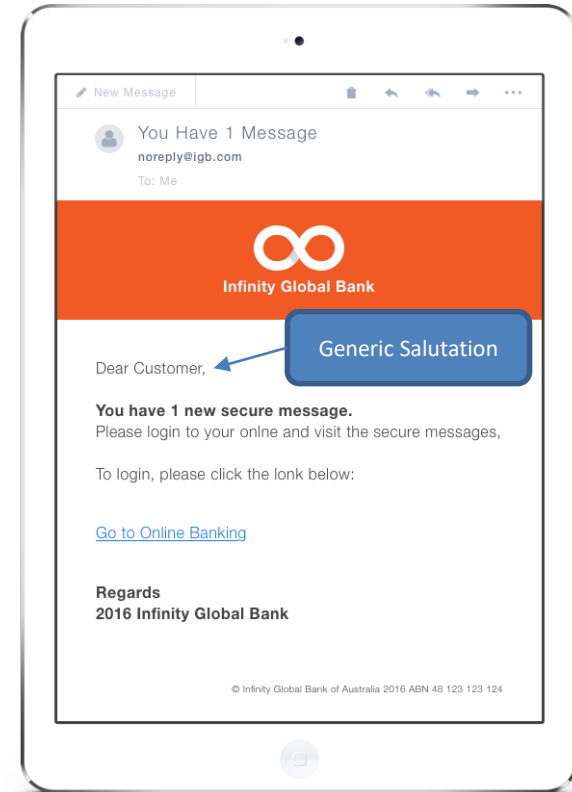
1. Just doesn't look right



Ten Tell-Tale Signs of Phishing

1. Just doesn't look right

2. Generic salutations



Ten Tell-Tale Signs of Phishing

1. Just doesn't look right

2. Generic salutations

3. Official-looking site asking you to enter sensitive data



Wed 02/26/2020 8:11 AM

MICROSOFT ACCOUNT TEAM <pom67@msn.com>

MICROSOFT ACCOUNT UPGRADE!!

To CPABC_infocusmag

[EXTERNAL EMAIL]



Microsoft Account

Dear user ID (infocusmag@bccpa.ca)

Request to disable your email has been received, and this request will be processed shortly. if you fail to upgrade to our new latest version within 24 hrs of receiving this automated mail, Please kindly take a minute and click the upgrade at your left to upgrade your E-mail....

Upgrade

<http://nimbus-shopping.com/XXX/home-office-updated/index.html?email=infocusmag@bccpa.ca>

Note: This upgrade is required immediately after receiving this message.....

Thanks .

Your Maintenance team

© Microsoft 2020.

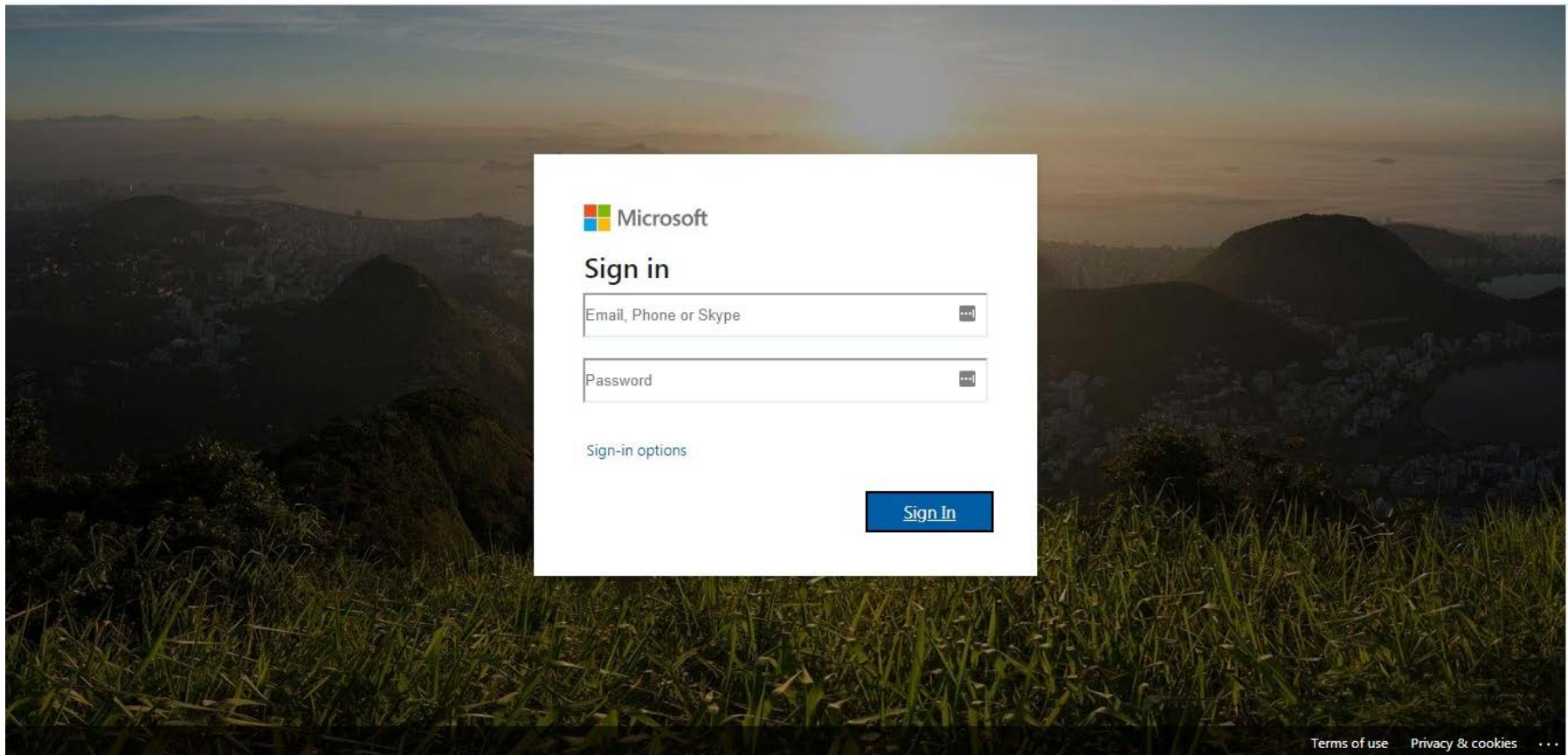
Important- Account disconnection will take place on 26th February 12:00 Midnight if issue not resolved.

Message sent to this recipient: infocusmag@bccpa.ca



Microsoft

Trying to Add A Sense of Urgency



Microsoft

Sign in

Email, Phone or Skype

Password

Sign-in options

[Sign In](#)

[Terms of use](#) [Privacy & cookies](#) ...

Ten Tell-Tale Signs of Phishing

1. Just doesn't look right

2. Generic salutations

3. Official-looking site asking you to enter sensitive data

4. Unexpected email; specific information on YOU

-----Original Message-----

From: CFO <michael.jaxon@no-protect.net>

To: John in Finance <john.smith@noproduct.net>

Subject: Urgent request

Hi John

Specific on you

Please call our supplier about wire payment details:
1.702.234.4567.

I'll be on a flight for the next 10 hours and unable
to take calls.

This is urgent!

Unexpected, from
Senior Manager

Best regards,

Michael
Protect Inc

Sent from my iPhone



Tue 02/25/2020 6:35 AM

Lori A. Mathison <richardpearson11111@gmail.com>

FAST ONE!!!

To Anthony Green

[EXTERNAL EMAIL]

Hello Anthony,

Specific on you

Would it be possible for you to complete a task for me,
before I leave for a meeting?

Please give me your personal number

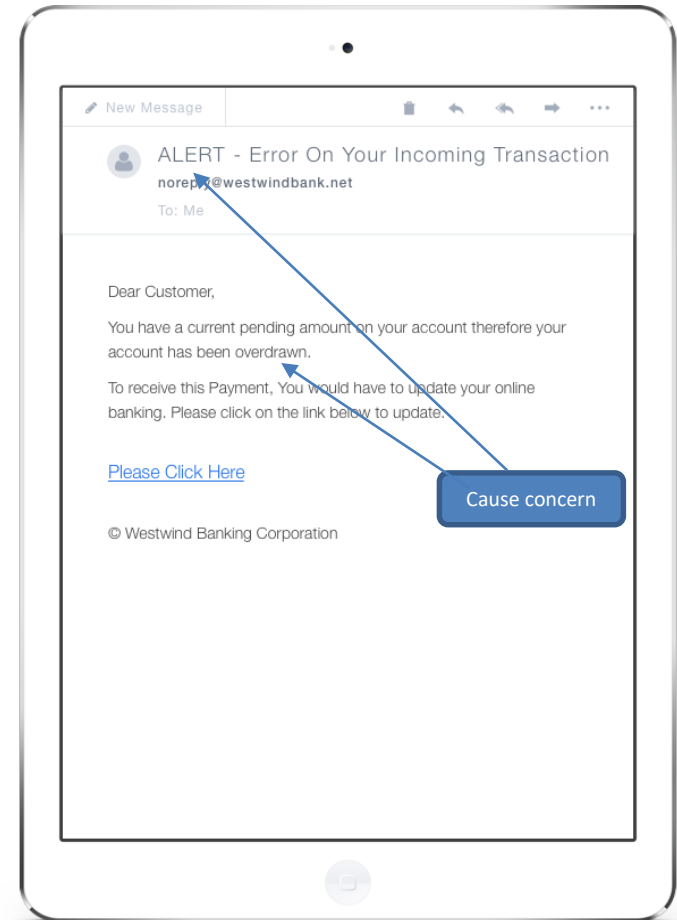
Thanks,
Lori A. Mathison

Unexpected from Senior Manager

Sent from my Iphone

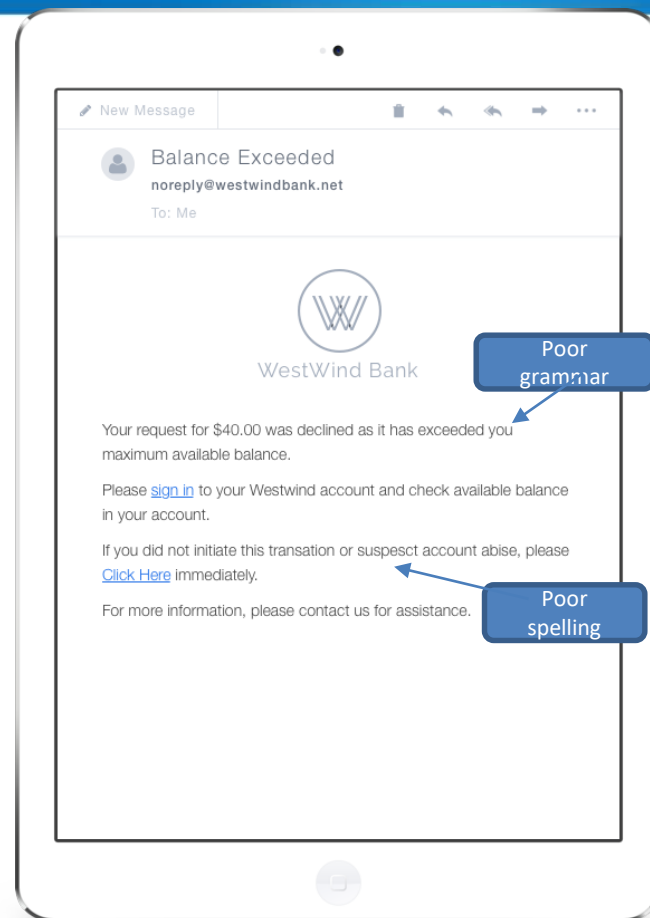
Ten Tell-Tale Signs of Phishing

1. Just doesn't look right
2. Generic salutations
3. Official-looking site asking you to enter sensitive data
4. Unexpected email; specific information on YOU
5. Unnerving wording



Ten Tell-Tale Signs of Phishing

1. Just doesn't look right
2. Generic salutations
3. Official-looking site asking you to enter sensitive data
4. Unexpected email; specific information on YOU
5. Unnerving wording
6. Poor grammar or spelling (or both)



Ten Tell-Tale Signs of Phishing

1. Just doesn't look right
2. Generic salutations
3. Official-looking site asking you to enter sensitive data
4. Unexpected email; specific information on YOU
5. Unnerving wording
6. Poor grammar or spelling (or both)
7. Sense of urgency



CPABC Support <support@bccpa.ca>

Important: pubprac@bccpa.ca You have 5 Pending incoming emails.

To BCCPA Public Practice

If there are problems with how this message is displayed, click here to view it in a web browser.

bccpa.ca Cloud Service

You have {5} undelivered mails clustered on your cloud due to mail storage capacity is full and awaiting approval from you to deliver messages and restore cloud storage. :

Be notified, this will make messages bounce back.:

Follow the instruction to resolve issue and release pending messages to inbox.

Release Messages

Thanks.

This email was sent to pubprac@bccpa.ca.

Ten Tell-Tale Signs of Phishing

1. Just doesn't look right
2. Generic salutations
3. Official-looking site asking you to enter sensitive data
4. Unexpected email; specific information on YOU
5. Unnerving wording
6. Poor grammar or spelling (or both)
7. Sense of urgency
8. "You've won the grand prize" or take survey

Survey with incentive

TESCO

Heres your chance to receive a
£300 TESCO CLUBCARD VOUCHER

Just simply answer our survey below to qualify:

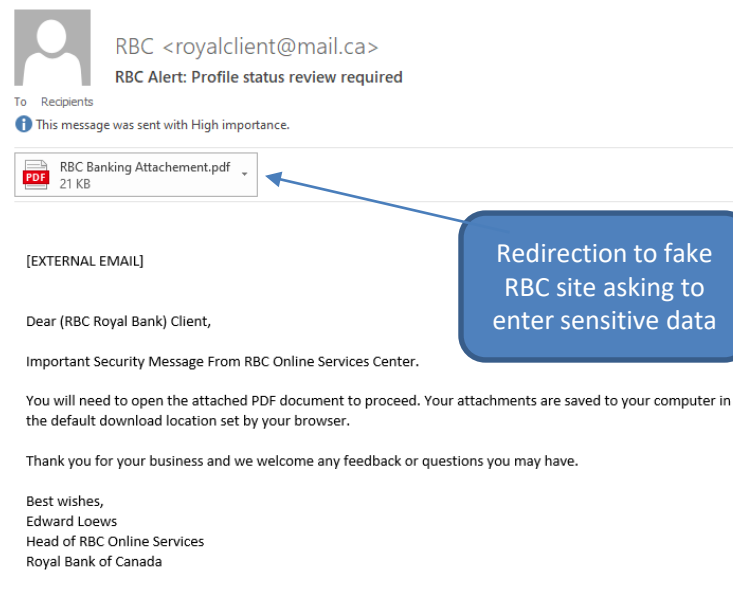
Which dishwashing liquid do you use often?

Tesco Wash Up Liquid
Fairy Washing Up Liquid
Finish Diswasher Cleaner

Tesco is a British multinational grocery and general merchandise retailer with headquarters in Welwyn Garden City, Hertfordshire, England, United Kingdom. It is the third largest retailer in the world measured by profits and fifth-largest retailer in the world measured by revenues.

Ten Tell-Tale Signs of Phishing

1. Just doesn't look right
2. Generic salutations
3. Official-looking site asking you to enter sensitive data
4. Unexpected email; specific information on YOU
5. Unnerving wording
6. Poor grammar or spelling (or both)
7. Sense of urgency
8. "You've won the grand prize"
9. "Verify your account"



Ten Tell-Tale Signs of Phishing

1. Just doesn't look right
2. Generic salutations
3. Official-looking site asking you to enter sensitive data
4. Unexpected email; specific information on YOU
5. Unnerving wording
6. Poor grammar or spelling (or both)
7. Sense of urgency
8. "You've won the grand prize"
9. "Verify your account"
10. Cybersquatting

www.bccpa.ca

vs.

www.cpabc.ca