Securing your Research on Compute Canada Clusters and Clouds
Day 2

Prepared by:
Raphaelle Gauriau
Information Systems Security Manager, SciNet

Agenda – Day 2

Review assignment 1

Best practices (suite)

Cryptography Concepts

SSH keys usage

Assignment 2

Assignment 1 - Review

Questions?

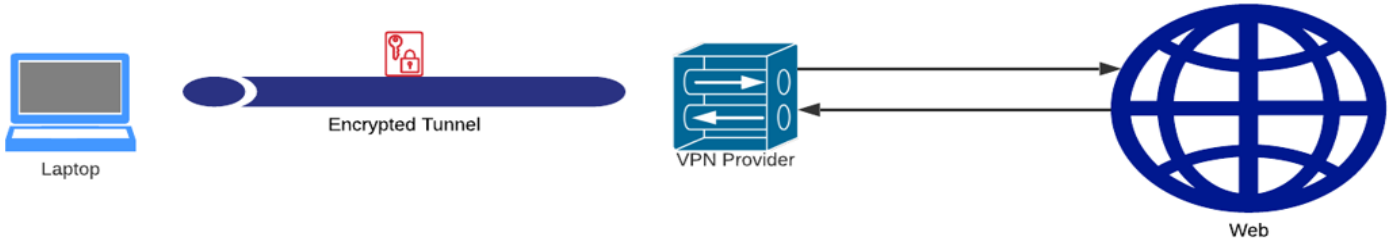
Findings?

Best Practices (suite)

End-Users

Virtual Private Network (VPN)

- **Encrypted connection** between the user's device and the Internet
- Provides online **privacy and anonymity** by masking the user's IP address
- Minimizes two main risks:
  - Privacy risk, as a VPN provides anonymity
  - Someone eavesdropping your connection
- Available **via your host institution**, or often included as part of anti-malware vendor service
- **Regulations** in some countries

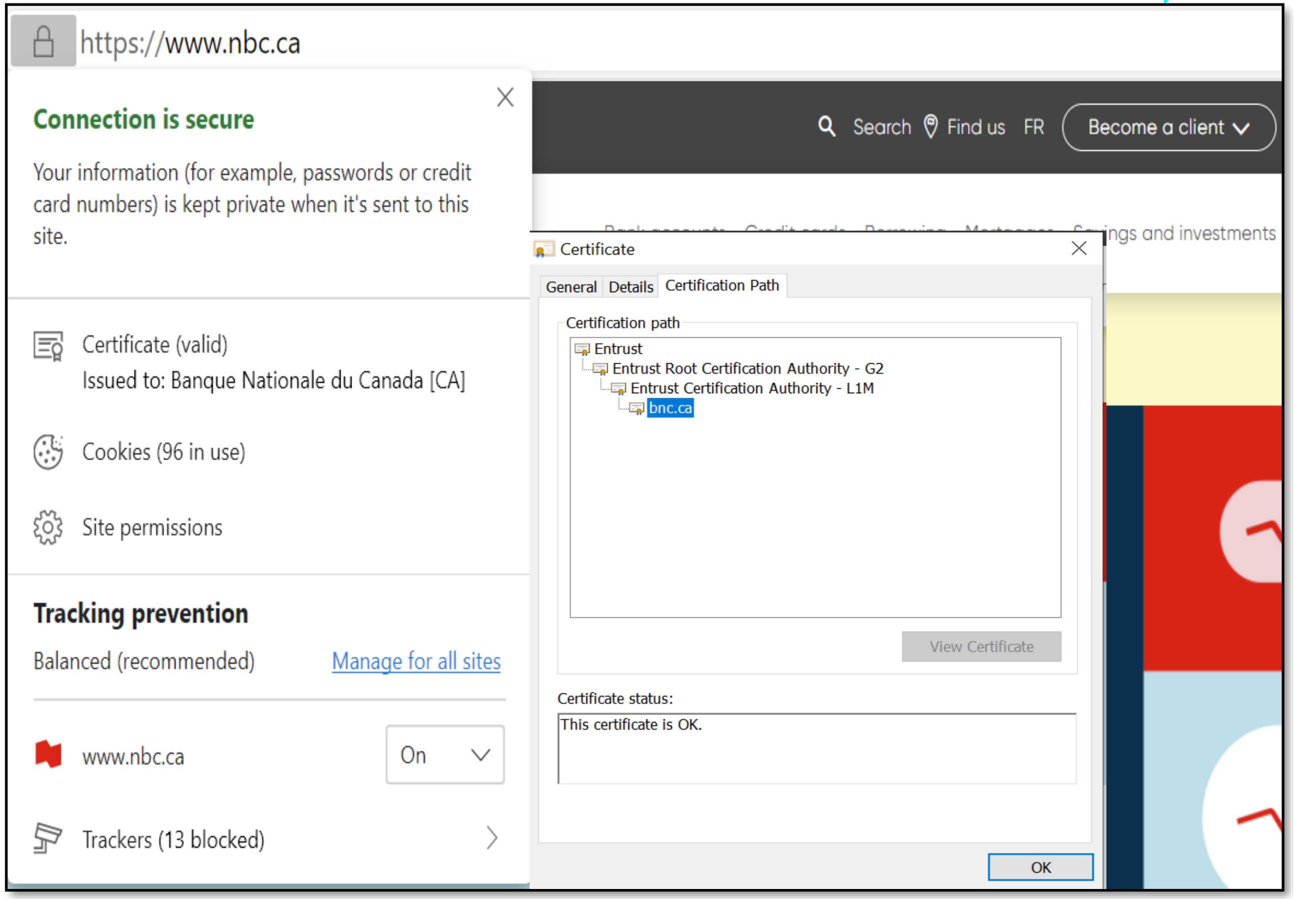


Best practice #3 - Safe Internet Browsing (1/2)

- **Public-WIFI**: **avoid** it as much as possible

- If you absolutely need to access a public WIFI:
  - Ensure that the WIFI name is known
  - Consider using a VPN (Virtual Private Network)
  - Stick to https websites and check certificates

- **Personal information**: be mindful of what you provide
  - Name, address, phone number, date of birth…



Connection is secure

Your information (for example, passwords or credit card numbers) is kept private when it's sent to this site.

Certificate (valid)
Issued to: Banque Nationale du Canada [CA]

Cookies (96 in use)

Site permissions

Tracking prevention

Balanced (recommended) Manage for all sites

www.nbc.ca On

Trackers (13 blocked)

Certificate

General | Details | Certification Path

Certification path

- Entrust
  - Entrust Root Certification Authority - G2
    - Entrust Certification Authority - L1M
      - bnc.ca

View Certificate

Certificate status:

This certificate is OK.

OK

Best practice #3 - Safe Internet Browsing (2/2)

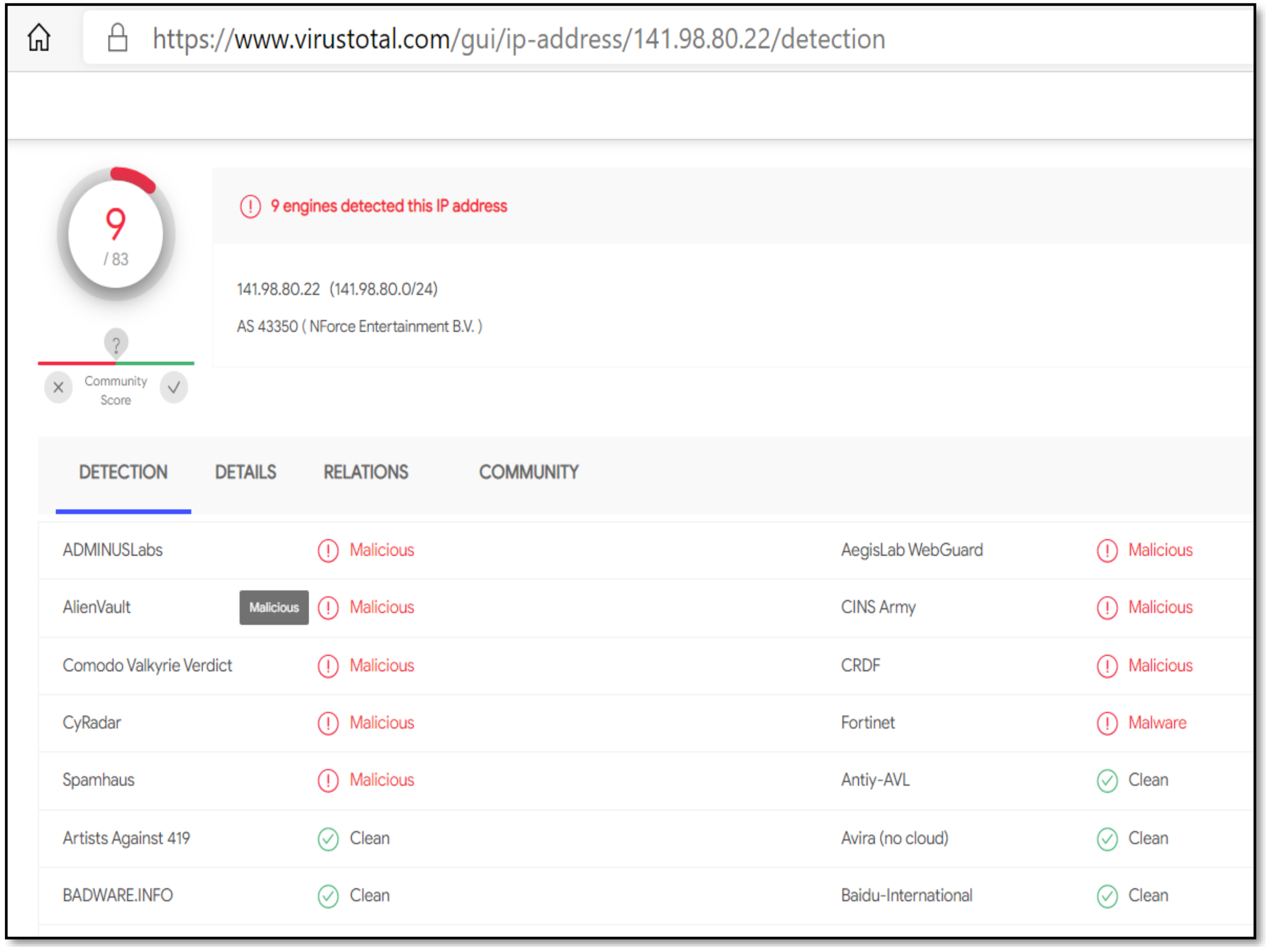
- Be careful with **browser extensions**

- Not sure about the **legitimacy** of a website?

  https://www.virustotal.com

- Use **Cira Canadian Shield** at home

  https://www.cira.ca/cybersecurity-services/canadian-shield



https://www.virustotal.com/gui/ip-address/141.98.80.22/detection

9 engines detected this IP address

141.98.80.22 (141.98.80.0/24)

AS 43350 (NForce Entertainment B.V.)

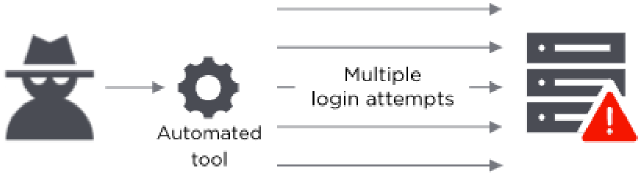
ADMINUSLabs	Malicious	AegisLab WebGuard	Malicious
AlienVault	Malicious	CINS Army	Malicious
Comodo Valkyrie Verdict	Malicious	CRDF	Malicious
CyRadar	Malicious	Fortinet	Malware
Spamhaus	Malicious	Antiy-AVL	Clean
Artists Against 419	Clean	Avira (no cloud)	Clean
BADWARE.INFO	Clean	Baidu-International	Clean

Anonymous Survey –

Do you use the same password to access different resources?

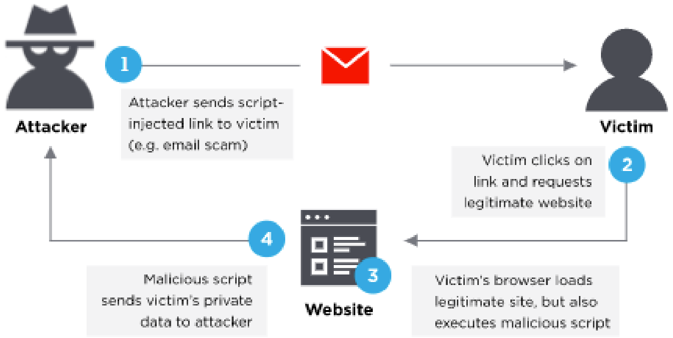
Passwords attacks (1/2)

- Brute force attacks



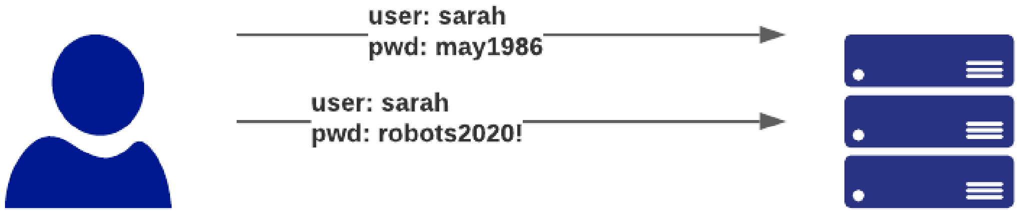
- Dictionary attacks

- Keyloggers


Attacker
1
Attacker sends script-injected link to victim (e.g. email scam)
Victim
Victim clicks on link and requests legitimate website
2
Website
3
Victim's browser loads legitimate site, but also executes malicious script
4
Malicious script sends victim's private data to attacker

Passwords attacks (2/2)

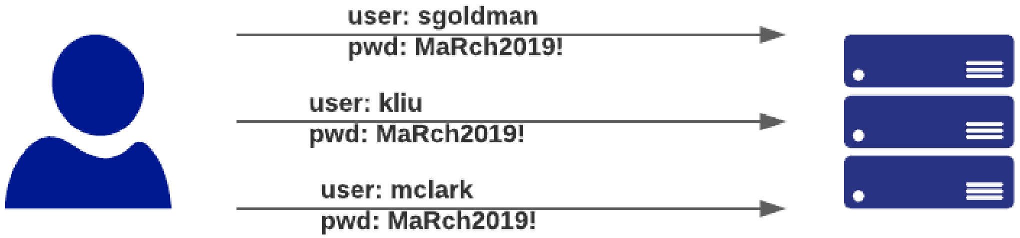
- Password guessing



user: sarah
pwd: may1986

user: sarah
pwd: robots2020!

- Password spraying



user: sgoldman
pwd: MaRch2019!

user: kliu
pwd: MaRch2019!

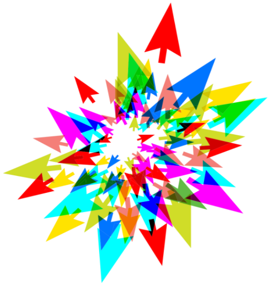
user: mclark
pwd: MaRch2019!

- Phishing

Best practice #4 - Password usage (1/2)

DO NOT

- Do not use the same password everywhere
- Do not use simple passwords (example: Summer2018)
- Do not store passwords in clear text
- Do not share your password
- Do not transmit password via email or text



Anonymous Survey –

Do you use a password vault?

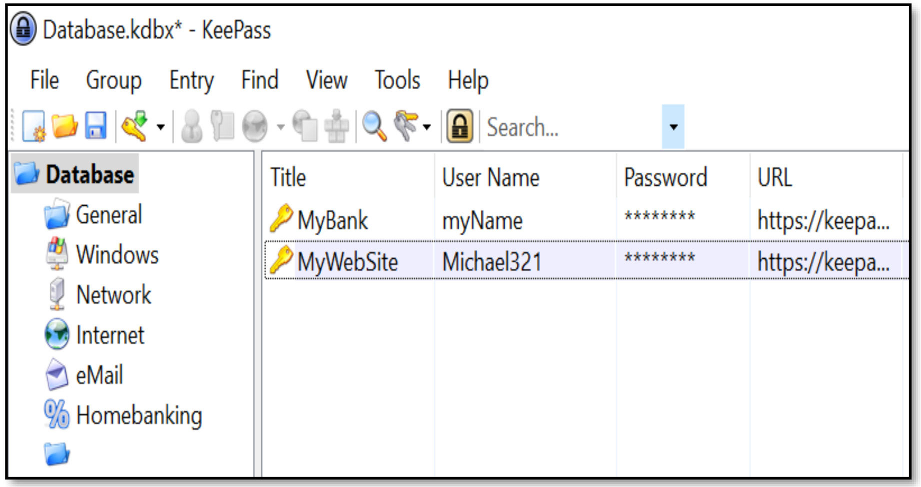
Best practice #4 - Password usage (2/2)

DO

- Use a different password for each account
- Use a password vault
  - LastPass
  - Keypass

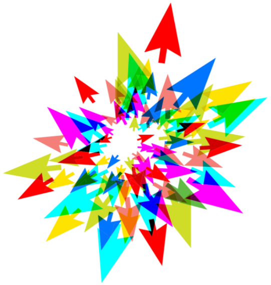
  Note 1: Dedicated password manager is usually more secure than storing your password in the browser

  Note 2: Ensure the master password is strong!
- Long passphrase (15 characters or more)
- Transmit securely
- Use MFA (multi-factor authentication) when possible



Title	User Name	Password	URL
MyBank	myName	********	https://keepa...
MyWebSite	Michael321	********	https://keepa...

Tips



Do you want to know if your personal information or password has been leaked?

Check this website:
https://haveibeenpwned.com/

Exercise 1

Install a password vault of your choice on your workstation and create one secret.

Please find below two options:

- Keypass

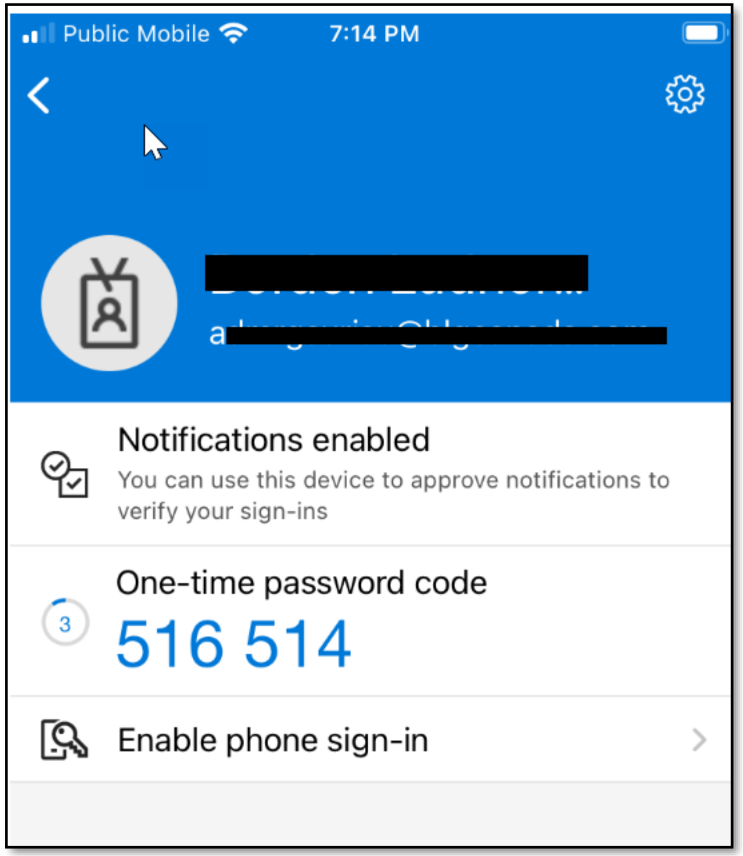
https://keepass.info/ (stored locally)

- LastPass

https://www.lastpass.com/ (stored in the Cloud)

Best practice #5 - Use MFA (1/2)

- Multi-Factor authentication: provide several pieces of evidence from different factors to prove your identity
- Factors:
  - Something you know
  - Something you have
  - Something you are
- Be careful when using your phone number as a second factor (ex: text message)
  - Phone number recycling



Public Mobile 7:14 PM

[redacted]

[redacted]

Notifications enabled

You can use this device to approve notifications to verify your sign-ins

One-time password code

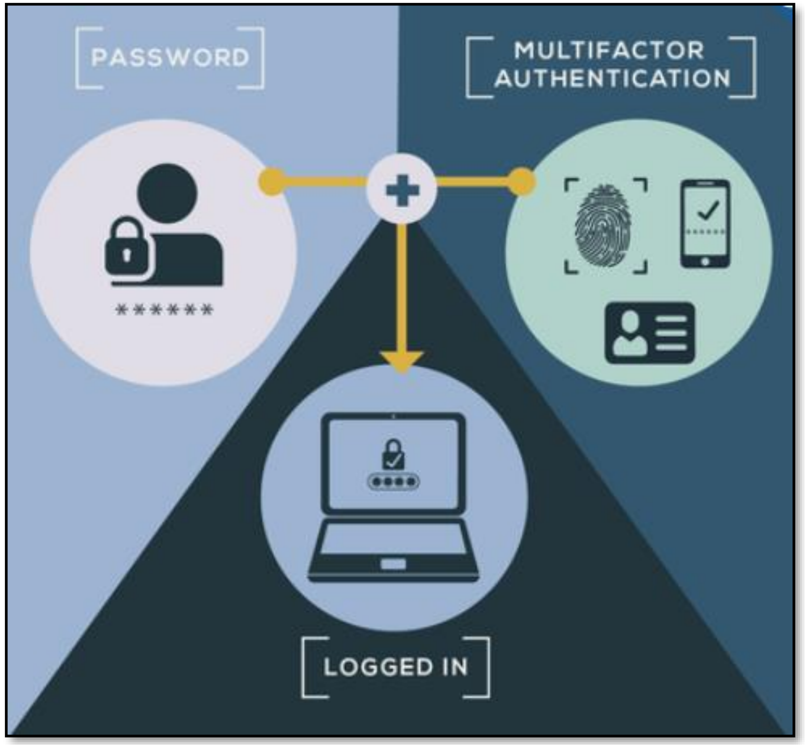
3

516 514

Enable phone sign-in

Best practice #5 - Use MFA (2/2)

- Protection against phishing, social engineering and password brute-force attacks and stolen credentials
- MFA pilot at Compute Canada
- Note: entering two different passwords is NOT considered as multi-factor



Source: https://www.nist.gov/itl/applied-cybersecurity/tig/back-basics-multi-factor-authentication

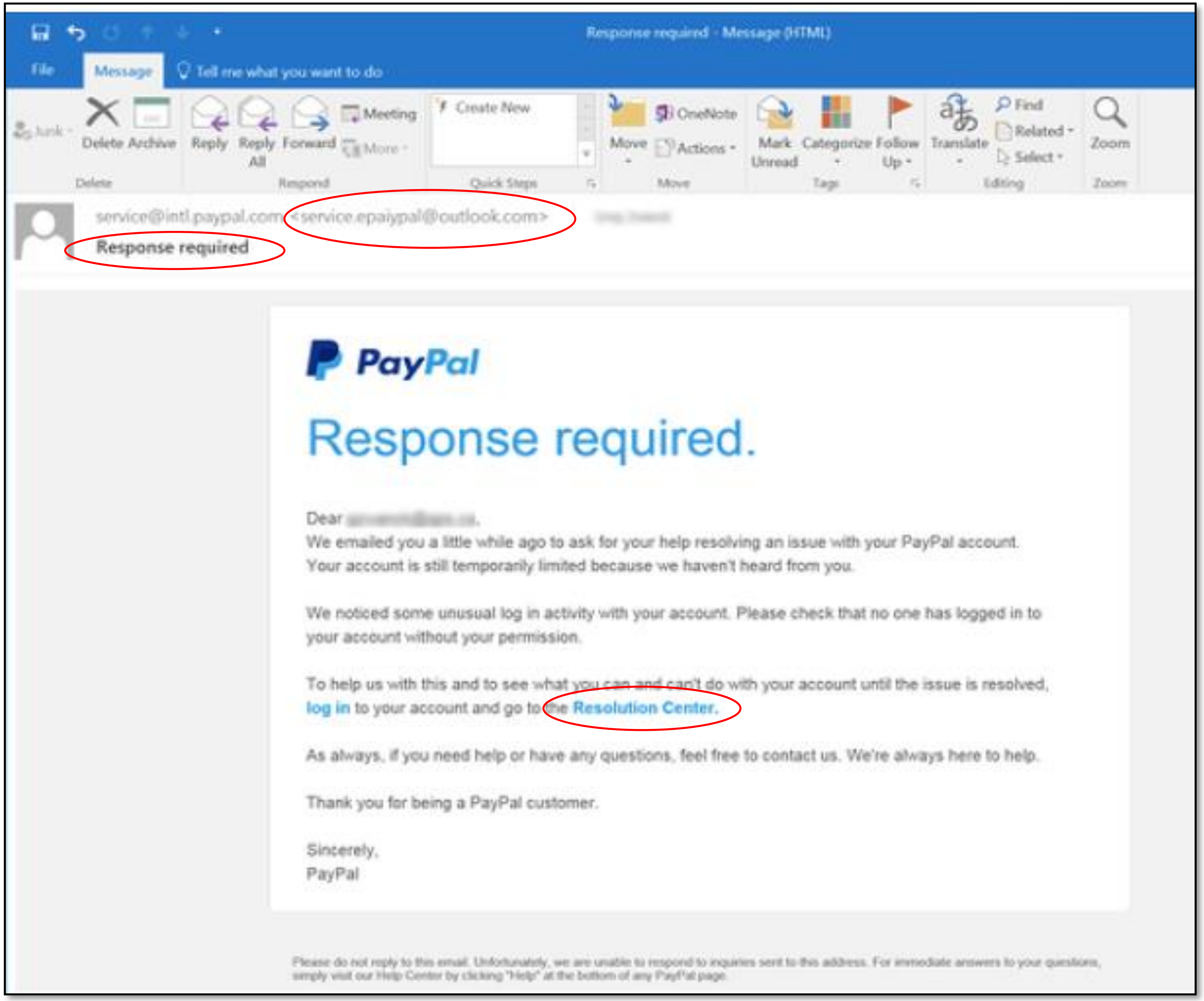
Best practice #6 - Be careful of phishing

- One of the most popular vector of attack

- Indicators of phishing:
  1. An Unfamiliar Tone or Greeting
  2. Grammar and Spelling Errors
  3. Inconsistencies in Email Addresses, Links & Domain Names
  4. Threats or a Sense of Urgency
  5. Suspicious Attachments

- In doubt: contact the sender via other means, or ask your home institution's security team

Sources: https://cofense.com/knowledge-center/signs-of-a-phishing-email/
https://www.pexels.com/photo/man-in-red-shirt-wearing-black-framed-eyeglasses-3965246/



service@intl.paypal.com<service.epaiypal@outlook.com> [redacted]

Response required

PayPal

Response required.

Dear [redacted].

We emailed you a little while ago to ask for your help resolving an issue with your PayPal account. Your account is still temporarily limited because we haven't heard from you.

We noticed some unusual log in activity with your account. Please check that no one has logged in to your account without your permission.

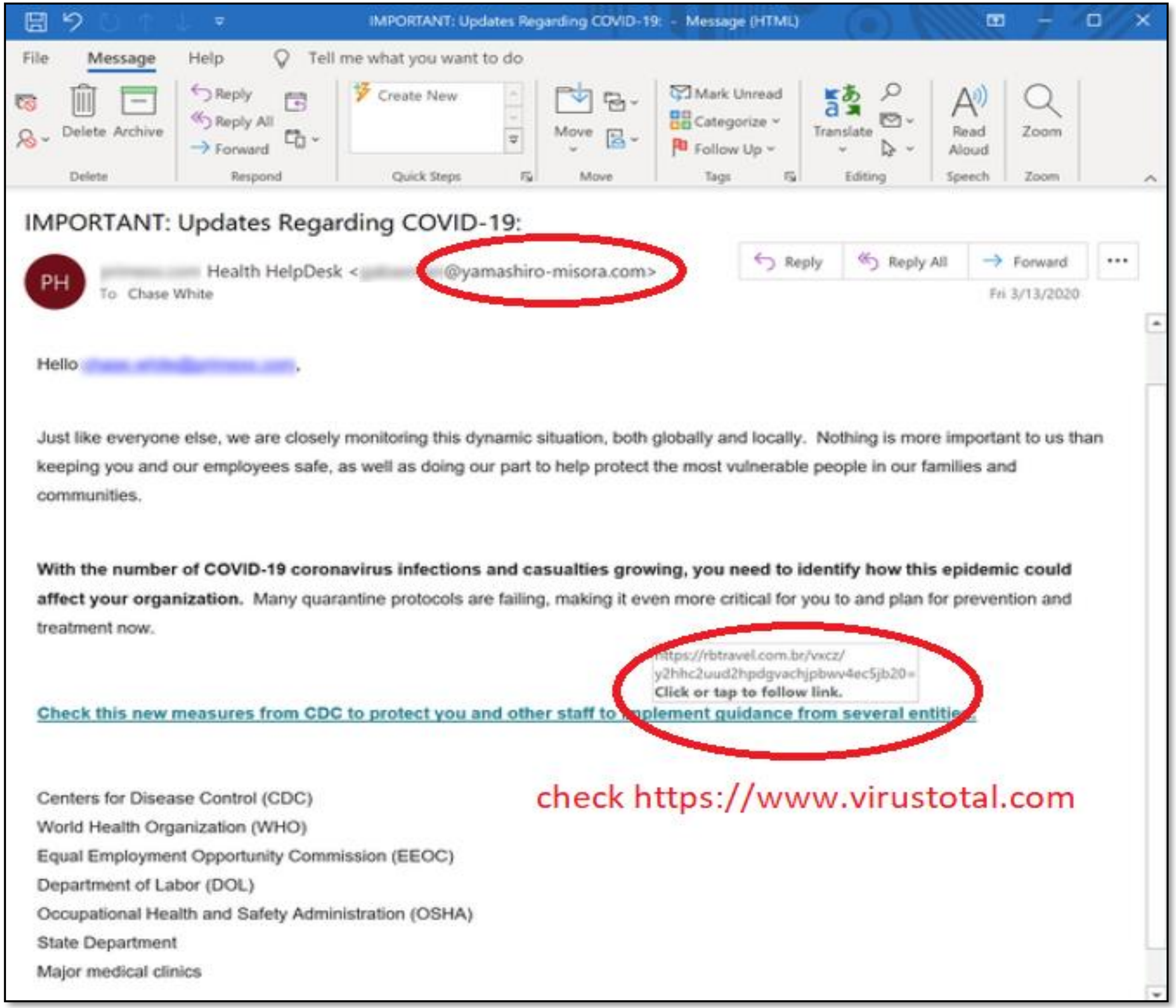
To help us with this and to see what you can and can't do with your account until the issue is resolved, log in to your account and go to the Resolution Center.

As always, if you need help or have any questions, feel free to contact us. We're always here to help.

Thank you for being a PayPal customer.

Sincerely,
PayPal

Please do not reply to this email. Unfortunately, we are unable to respond to inquiries sent to this address. For immediate answers to your questions, simply visit our Help Center by clicking "Help" at the bottom of any PayPal page.



IMPORTANT: Updates Regarding COVID-19:

[redacted] Health HelpDesk <[redacted]@yamashiro-misora.com>
To Chase White
Fri 3/13/2020

Hello [redacted].

Just like everyone else, we are closely monitoring this dynamic situation, both globally and locally. Nothing is more important to us than keeping you and our employees safe, as well as doing our part to help protect the most vulnerable people in our families and communities.

With the number of COVID-19 coronavirus infections and casualties growing, you need to identify how this epidemic could affect your organization. Many quarantine protocols are failing, making it even more critical for you to and plan for prevention and treatment now.

https://rbtravel.com.br/vxcz/
y2hhc2uud2hpdgvachjpbwv4ec5jb20=
Click or tap to follow link.

Check this new measures from CDC to protect you and other staff to implement guidance from several entities.

check https://www.virustotal.com

Centers for Disease Control (CDC)
World Health Organization (WHO)
Equal Employment Opportunity Commission (EEOC)
Department of Labor (DOL)
Occupational Health and Safety Administration (OSHA)
State Department
Major medical clinics

Best practice #6 - Backup your data (1/3)

- **Data loss** can occur due to incidents like **power surge, cyberattacks like ransomware, physical theft**
- **Backup** your important data **on a regular basis**
- Keep your backups in **a safe, different location**
- Cloud vs on-premise
- **Test** your backups!

Best practice #6 - Backup your data (2/3)

Different types of backups

- ***Full backups***: most applicable in the context of a user
- ***Incremental backups***: store only those files that have been modified since the time of the most recent full or incremental backup. Saves time and space. Applicable in the context of an organization.
- ***Differential backups***: store all files that have been modified since the time of the most recent full backup. Saves time and space. Applicable in the context of an organization.

Best practice #6 - Backup your data (3/3)

On **CC** systems (**non cloud**):

- $HOME and $PROJECT are backed up

On **CC** systems (**cloud**):

- Your responsibility

https://docs.computecanada.ca/wiki/Backing_up_your_VM/en

Cryptography

& SSH keys

Cryptography Definitions

Encryption: The process of converting the message from its plaintext to ciphertext

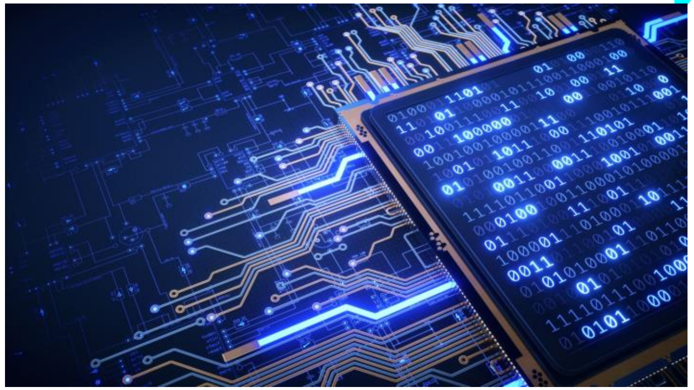
Plaintext: The message in its natural format has not been turned into a secret.

Ciphertext: The altered form of a plaintext message, so as to be unreadable for anyone except the intended recipients. Something that has been turned into a secret.

Hash function: Accepts an input message of any length and generates, through a one-way operation, a fixed-length output called a message digest or hash (ex: SHA-256).
<u>Example of use case</u>: data integrity

Source: https://www.isc2.org/Certifications/CISSP/CISSP-Student-Glossary

Encryption – Why? Where?



Why:

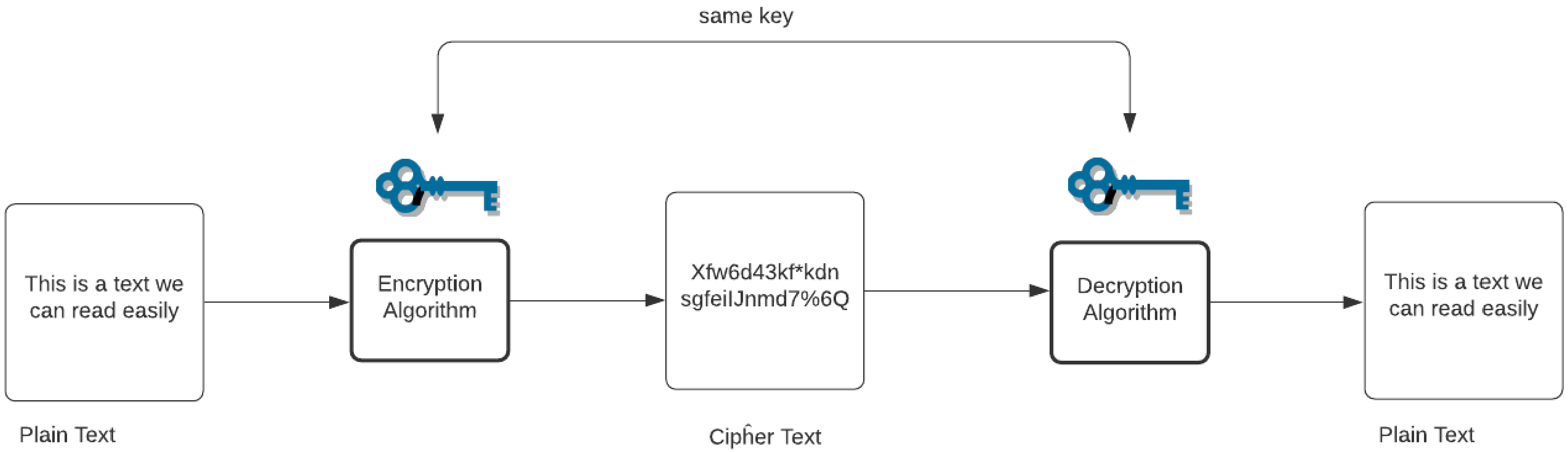
- Protect sensitive data

What :

- **In transit**
  - Data moving from one location to another (HTTPS, SSL, TLS, FTPS, etc)
  - Attacks against data in transit include man-in-the-middle attacks, wired tapping
- **At rest**
  - Data stored on a hard drive, laptop, flash drive, or archived/stored in some other way
  - Attacks against data at-rest include attempts to obtain physical access to the hardware on which the data is stored, and then compromise the contained data.
  - Requirement by some regulations: HIPAA, PCI

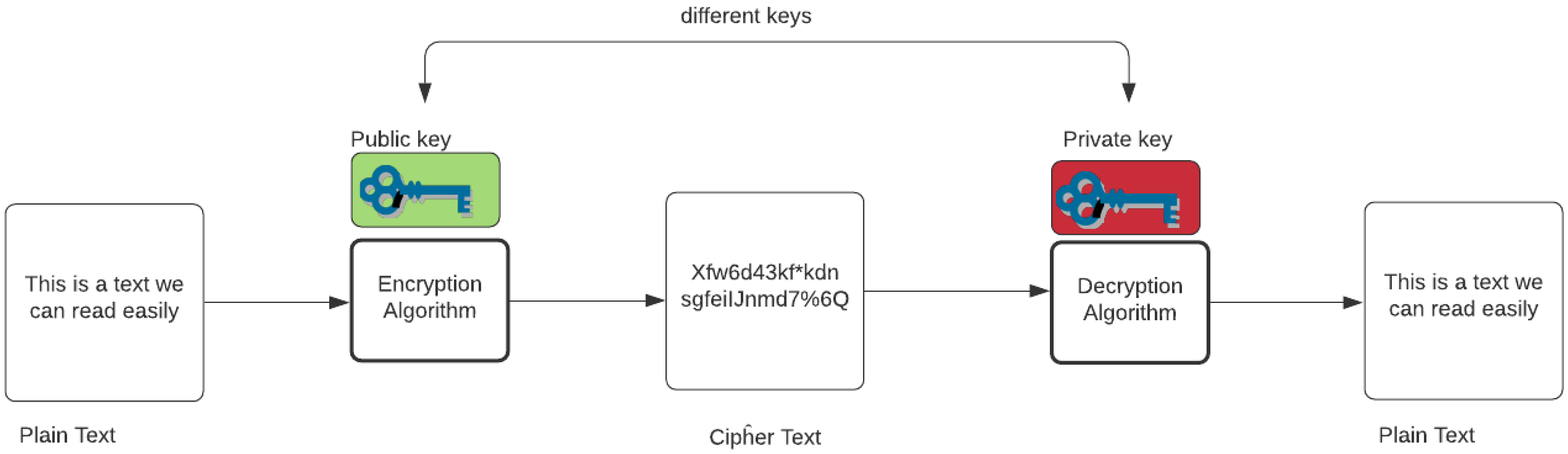
Symmetric vs Asymmetric Encryption (1/3)

Symmetric


same key
This is a text we can read easily
Encryption Algorithm
Xfw6d43kf*kdn sgfeilJnmd7%6Q
Decryption Algorithm
This is a text we can read easily
Plain Text
Cipher Text
Plain Text

Symmetric vs Asymmetric Encryption (2/3)

Asymmetric



Symmetric vs Asymmetric Encryption (3/3)

Symmetric encryption

One secret key to encrypt and decrypt

Very efficient

How do you exchange the secret key?

Algorithms:
RC4*, AES, DES*, 3DES, QUAD, Blowfish

*: weak algorithms

Asymmetric encryption

One key to encrypt, another key to decrypt

Public key vs Private key

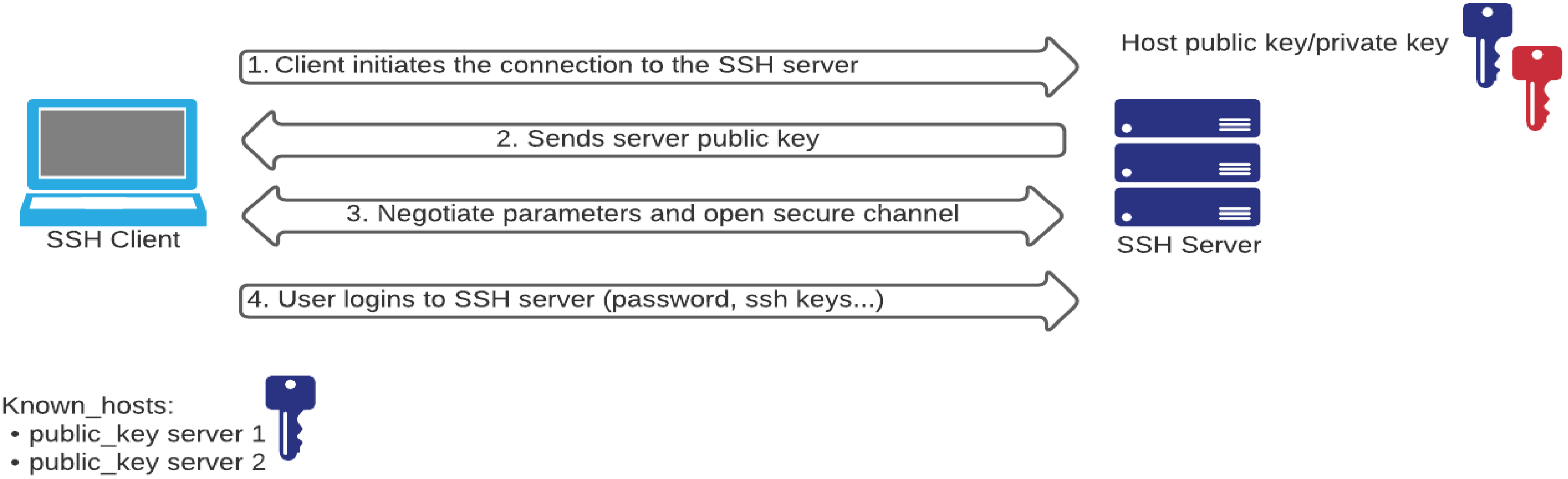
Public key: available to everyone

Private key: keep in a secure location

Algorithms:
RSA, Diffie-Hellman, ECC

Real-Life Scenario: SSH

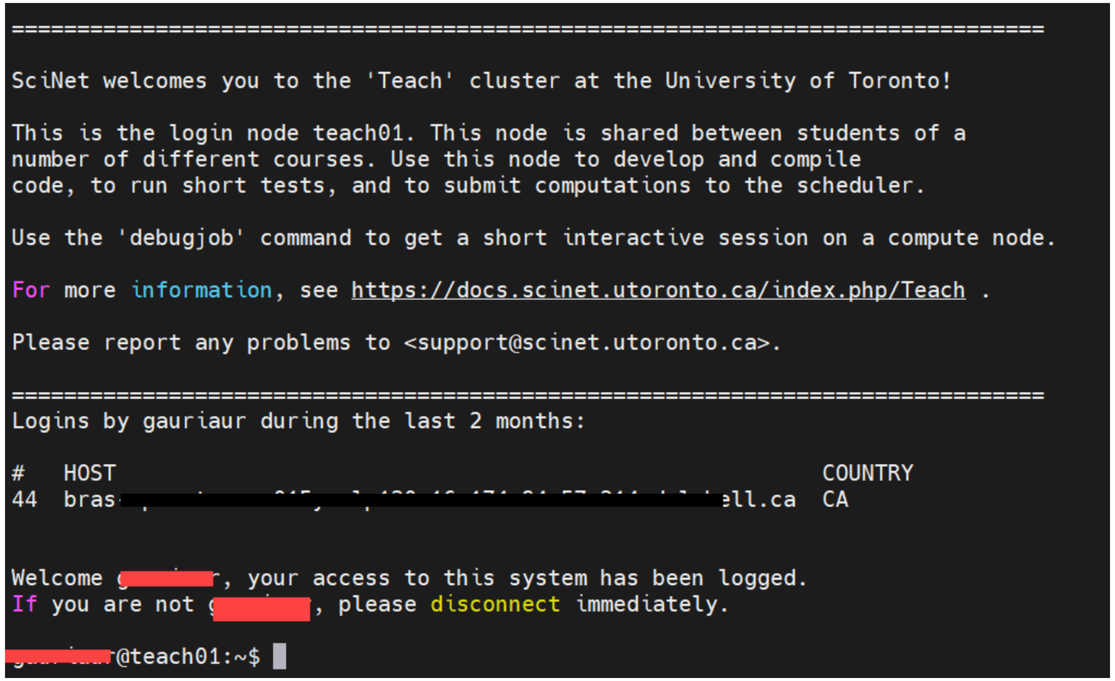
SSH (Secure Shell): a method for secure remote login


1. Client initiates the connection to the SSH server
Host public key/private key
SSH Client
2. Sends server public key
3. Negotiate parameters and open secure channel
SSH Server
4. User logins to SSH server (password, ssh keys...)
Known_hosts:
• public_key server 1
• public_key server 2

Exercise 2

Authenticate to Teach SSH server via a password

teach.scinet.utoronto.ca



```
==============================================================================

SciNet welcomes you to the 'Teach' cluster at the University of Toronto!

This is the login node teach01. This node is shared between students of a
number of different courses. Use this node to develop and compile
code, to run short tests, and to submit computations to the scheduler.

Use the 'debugjob' command to get a short interactive session on a compute node.

For more information, see https://docs.scinet.utoronto.ca/index.php/Teach .

Please report any problems to <support@scinet.utoronto.ca>.

==============================================================================
Logins by gauriaur during the last 2 months:

#   HOST                                                        COUNTRY
44  bras[redacted]ell.ca  CA


Welcome [redacted], your access to this system has been logged.
If you are not [redacted], please disconnect immediately.

[redacted]@teach01:~$ █
```

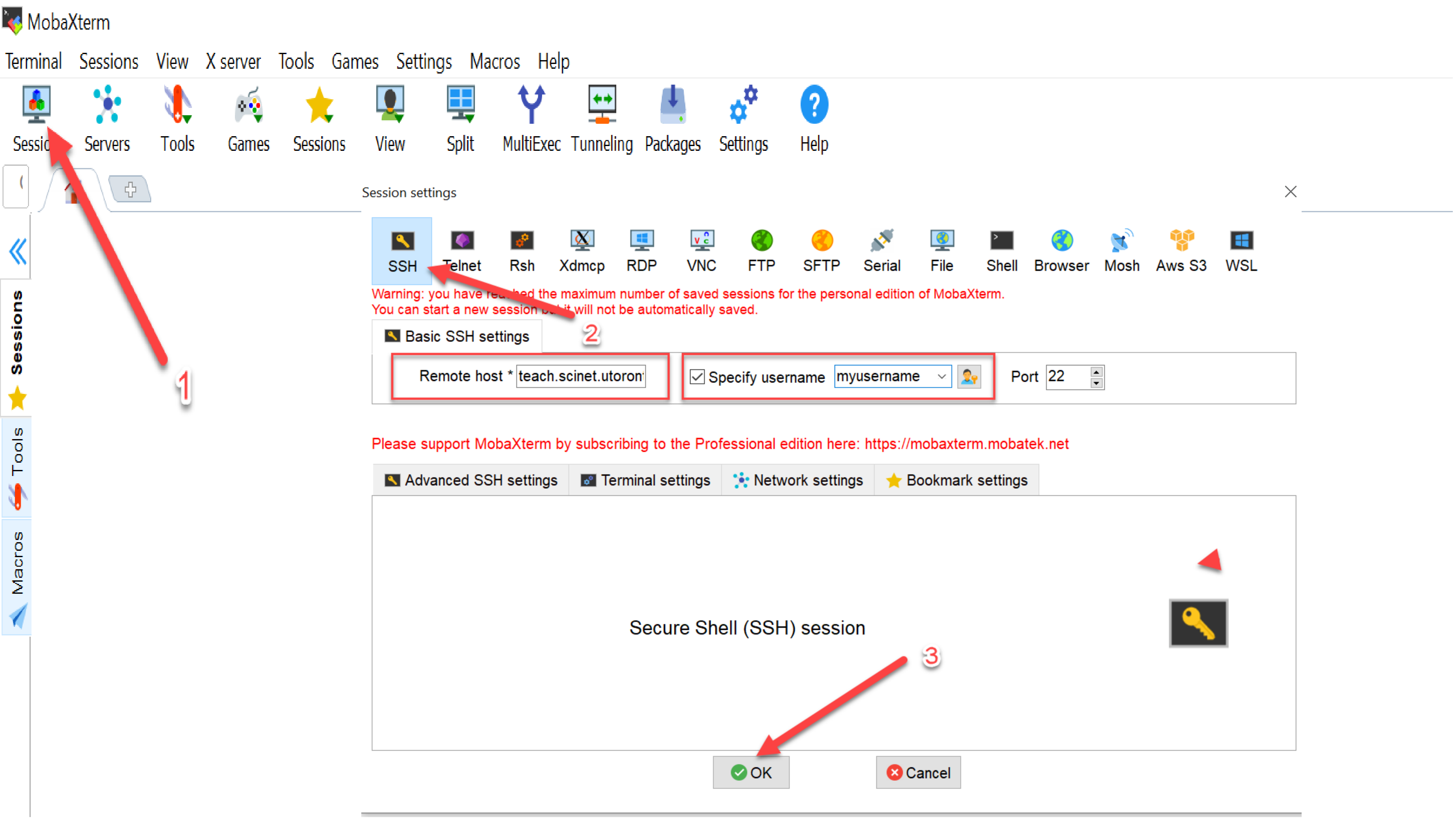
Windows:

Use MobaXterm

MacOS/Linux:

Via a terminal, type:

ssh username@teach.scinet.utoronto.ca



MobaXterm
Terminal Sessions View X server Tools Games Settings Macros Help
Sessio Servers Tools Games Sessions View Split MultiExec Tunneling Packages Settings Help
Sessions
Tools
Macros
Session settings
SSH Telnet Rsh Xdmcp RDP VNC FTP SFTP Serial File Shell Browser Mosh Aws S3 WSL
Basic SSH settings
Advanced SSH settings
Terminal settings
Network settings
Bookmark settings
Secure Shell (SSH) session
OK
Cancel
1
2
3

Warning: you have reached the maximum number of saved sessions for the personal edition of MobaXterm.
You can start a new session but it will not be automatically saved.

Remote host * teach.scinet.utoron

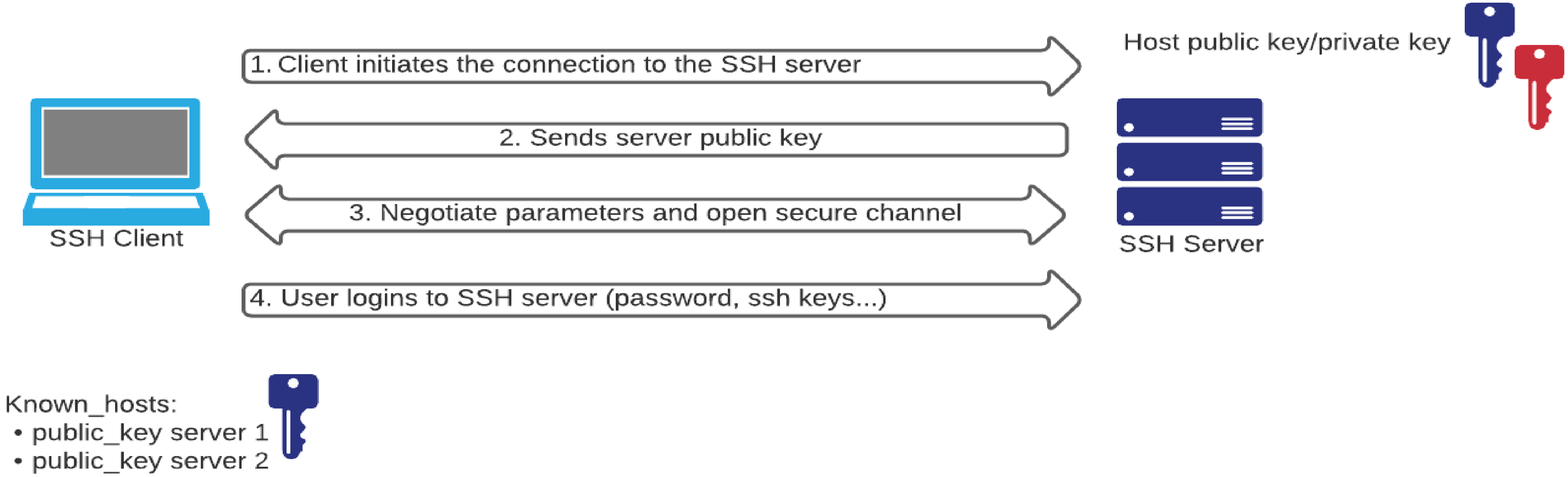
☑ Specify username myusername

Port 22

Please support MobaXterm by subscribing to the Professional edition here: https://mobaxterm.mobatek.net

Real-Life Scenario: SSH

SSH (Secure Shell): a method for secure remote login



Host public key/private key

1. Client initiates the connection to the SSH server

2. Sends server public key

3. Negotiate parameters and open secure channel

4. User logins to SSH server (password, ssh keys...)

Known_hosts:

- public_key server 1
- public_key server 2

SSH keys for authentication

- SSH keys: an alternative to passwords to authenticate
- Harder to crack than passwords
- Private key vs public key
- Protect your **private key in a safe location**
- **Do not share your private key!**
- Add a **passphrase** to the private key

Strength	RSA	ECDSA, EdDSA, DH, MQV
NOT RECOMMENDED ANYMORE	k = 1024	f = 160-223
RECOMMENDED	k = 2048 (and above)	f = 224-255 (and above)

Note: k and f above are commonly considered as key size

Asymmetric Algorithms and Corresponding Keys

Source: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57pt1r5.pdf

Anonymous Survey –

Have you created an SSH key pair before?

Exercise 3

<u>**Goal**</u>: Create an SSH key pair on your workstation, then authenticate to SciNet Teach cluster via SSH key.

STEP 1 – <u>On your workstation</u>, create your SSH key pair.

STEP 2 – Make the public key available on Teach cluster.

Option a – Upload the SSH **public** key to CCDB (Compute Canada account needed):

https://ccdb.computecanada.ca/ssh_authorized_keys

Option b - Copy the SSH public key to Teach, under .ssh/authorized_keys file

STEP 3 – From your workstation, try to authenticate to Teach with your SSH key.

Source: https://docs.computecanada.ca/wiki/SSH_Keys

STEP 1 – Create your SSH Key pair

Steps for **Linux/MacOS**:
https://docs.computecanada.ca/wiki/Using_SSH_keys_in_Linux

Steps for **Windows**:
https://docs.computecanada.ca/wiki/Generating_SSH_keys_in_Windows

Recommendations:

- Add a passphrase to encrypt the private key; 15 characters or more.
- Name the SSH key as you may create SSH keys for other systems. Ex: LaptopName_CC_id_ed25519
- If you have several laptops, create dedicated SSH key pairs for each of them.

STEP 2 – Make the public key available on Teach cluster

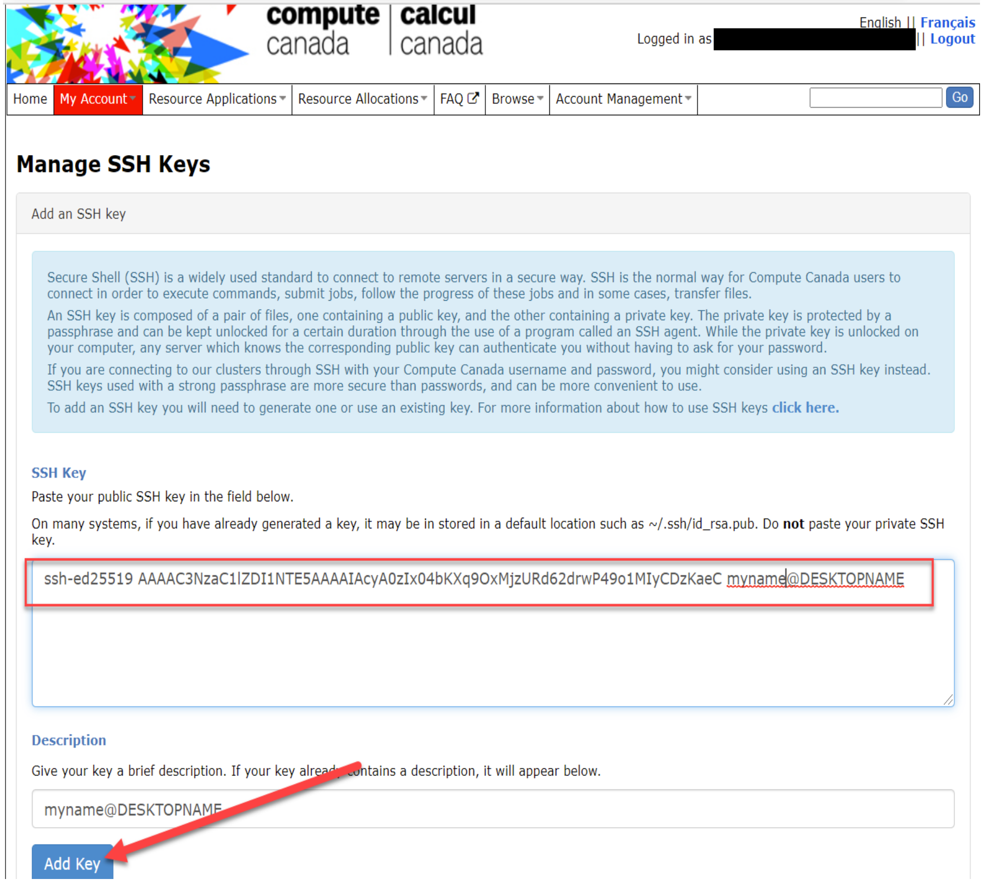
Option a - Upload the SSH **public** key to CCDB (Compute Canada account needed):

https://ccdb.computecanada.ca/ssh_authorized_keys

Option b - Copy the SSH **public** key to Teach, under .ssh/authorized_keys file

https://docs.computecanada.ca/wiki/Using_SSH_keys_in_Linux#Installing_locally

https://docs.computecanada.ca/wiki/Generating_SSH_keys_in_Windows#Installing_locally



Logged in as [redacted]

Manage SSH Keys

Add an SSH key

Secure Shell (SSH) is a widely used standard to connect to remote servers in a secure way. SSH is the normal way for Compute Canada users to connect in order to execute commands, submit jobs, follow the progress of these jobs and in some cases, transfer files.

An SSH key is composed of a pair of files, one containing a public key, and the other containing a private key. The private key is protected by a passphrase and can be kept unlocked for a certain duration through the use of a program called an SSH agent. While the private key is unlocked on your computer, any server which knows the corresponding public key can authenticate you without having to ask for your password.

If you are connecting to our clusters through SSH with your Compute Canada username and password, you might consider using an SSH key instead. SSH keys used with a strong passphrase are more secure than passwords, and can be more convenient to use.

To add an SSH key you will need to generate one or use an existing key. For more information about how to use SSH keys **click here.**

SSH Key

Paste your public SSH key in the field below.

On many systems, if you have already generated a key, it may be in stored in a default location such as ~/.ssh/id_rsa.pub. Do **not** paste your private SSH key.

```
ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIAcyA0zIx04bKXq9OxMjzURd62drwP49o1MIyCDzKaeC myname@DESKTOPNAME
```

Description

Give your key a brief description. If your key already contains a description, it will appear below.

myname@DESKTOPNAME

Option a – Upload public key to CCDB

Source: https://docs.computecanada.ca/wiki/SSH_Keys

STEP 3 – Authenticate with your SSH Key pair

From your workstation, authenticate to Teach with SSH key:

On Linux/MacOS:

```
$ ssh  -i   ~/.ssh/private_key_name   myusername@teach.scinet.utoronto.ca
```

On Windows:

https://docs.computecanada.ca/wiki/Connecting_with_PuTTY#Using_a_Key_Pair

https://docs.computecanada.ca/wiki/Connecting_with_MobaXTerm#Using_a_Key_Pair

Exercise 3

Goal: Create an SSH key pair on your workstation, then authenticate to SciNet Teach cluster via SSH key.

STEP 1 – On your workstation, create your SSH Key pair.

STEP 2 – Make the public key available on Teach cluster.

Option a – Upload the SSH **public** key to CCDB (Compute Canada account needed):

https://ccdb.computecanada.ca/ssh_authorized_keys

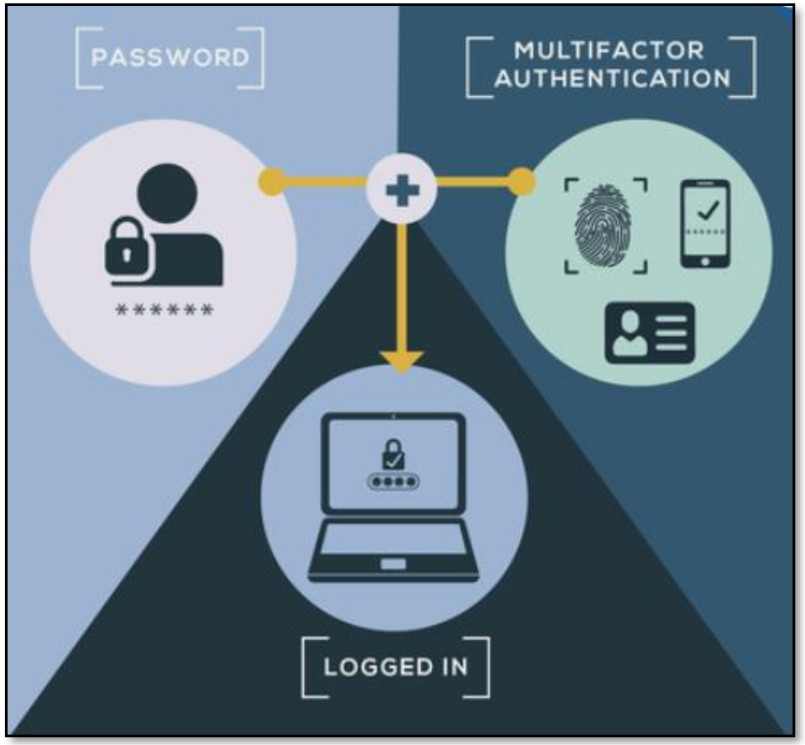
Option b - Copy the SSH public key to Teach, under .ssh/authorized_keys file

STEP 3 – From your workstation, try to authenticate to Teach with your SSH key.

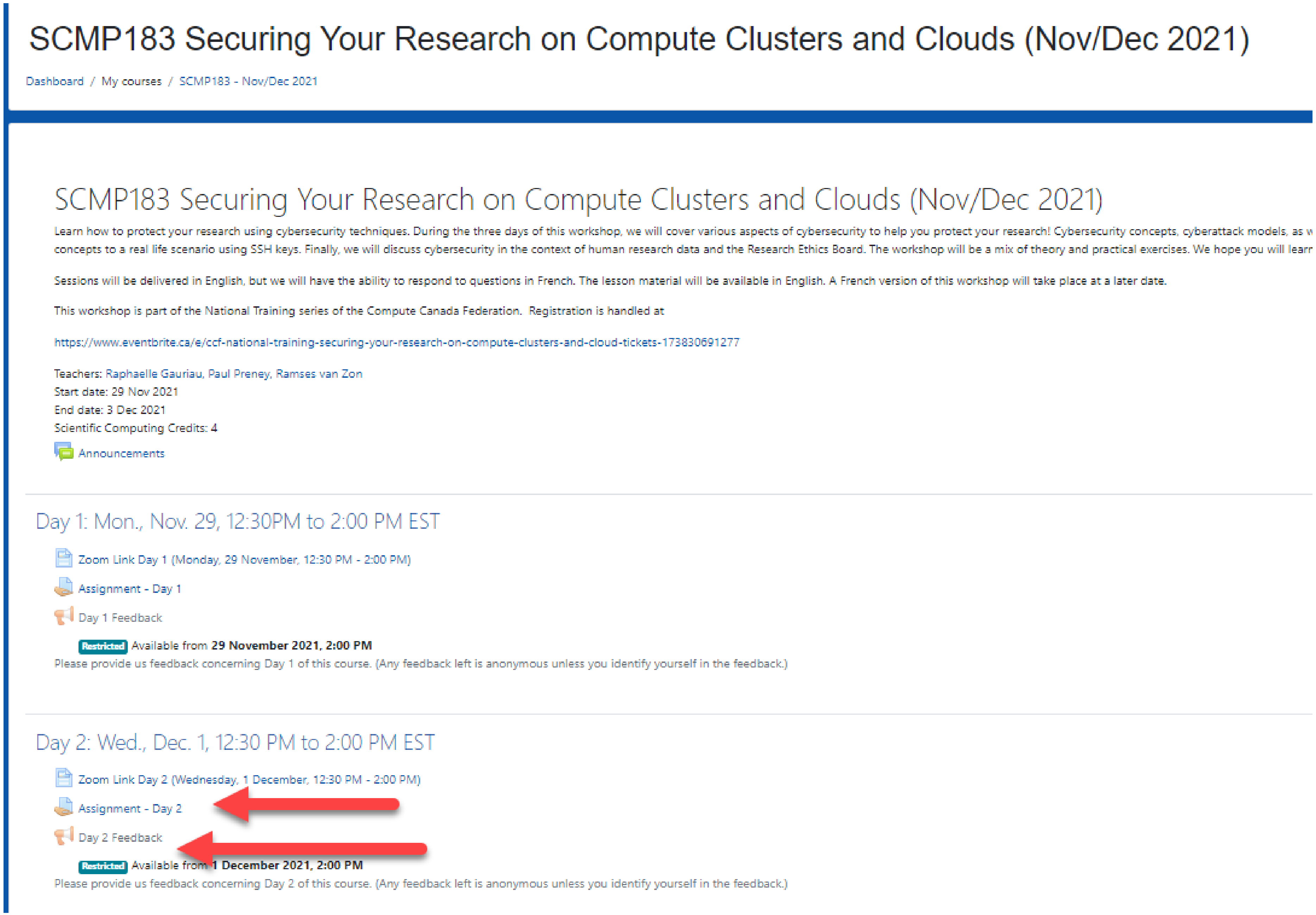
Source: https://docs.computecanada.ca/wiki/SSH_Keys

Key Take-Aways – Day 2

- Be mindful of **phishing**
- Use a **password vault**, combined with **MFA** whenever possible
- **Consider encryption** at rest and in transit to secure your data
- **Use SSH keys** and protect your SSH private key (location, passphrase)



Source: https://www.nist.gov/itl/applied-cybersecurity/tig/back-basics-multi-factor-authentication



SCMP183 Securing Your Research on Compute Clusters and Clouds (Nov/Dec 2021)

Dashboard / My courses / SCMP183 - Nov/Dec 2021

SCMP183 Securing Your Research on Compute Clusters and Clouds (Nov/Dec 2021)

Learn how to protect your research using cybersecurity techniques. During the three days of this workshop, we will cover various aspects of cybersecurity to help you protect your research! Cybersecurity concepts, cyberattack models, as w concepts to a real life scenario using SSH keys. Finally, we will discuss cybersecurity in the context of human research data and the Research Ethics Board. The workshop will be a mix of theory and practical exercises. We hope you will learr

Sessions will be delivered in English, but we will have the ability to respond to questions in French. The lesson material will be available in English. A French version of this workshop will take place at a later date.

This workshop is part of the National Training series of the Compute Canada Federation. Registration is handled at

https://www.eventbrite.ca/e/ccf-national-training-securing-your-research-on-compute-clusters-and-cloud-tickets-173830691277

Teachers: Raphaelle Gauriau, Paul Preney, Ramses van Zon
Start date: 29 Nov 2021
End date: 3 Dec 2021
Scientific Computing Credits: 4

Announcements

Day 1: Mon., Nov. 29, 12:30PM to 2:00 PM EST

Zoom Link Day 1 (Monday, 29 November, 12:30 PM - 2:00 PM)

Assignment - Day 1

Day 1 Feedback

Restricted Available from **29 November 2021, 2:00 PM**
Please provide us feedback concerning Day 1 of this course. (Any feedback left is anonymous unless you identify yourself in the feedback.)

Day 2: Wed., Dec. 1, 12:30 PM to 2:00 PM EST

Zoom Link Day 2 (Wednesday, 1 December, 12:30 PM - 2:00 PM)

Assignment - Day 2

Day 2 Feedback

Restricted Available from **1 December 2021, 2:00 PM**
Please provide us feedback concerning Day 2 of this course. (Any feedback left is anonymous unless you identify yourself in the feedback.)

Assignment – Day 2

1. What did you learn in today's session (1-2 items)?
2. Install a password vault and create some secrets (see Exercise 1).
3. Create an SSH key pair, then add your public key to Teach cluster and try to authenticate via SSH key (see Exercise 3).

Other resources

- https://securitymatters.utoronto.ca/resources/students/
- https://securityplanner.org/#/
- https://www.ic.gc.ca/eic/site/063.nsf/eng/h_97955.html

Sources and Images (day 1 and day 2)

- https://resources.infosecinstitute.com/certification/the-cissp-domains-an-overview/
- https://cyber.gc.ca/en/guidance/cyber-threat-and-cyber-threat-actors
- https://www.nist.gov/itl/smallbusinesscyber/cybersecurity-basics/glossary
- https://www.avast.com/en-ca/business/resources/defence-in-depth
- https://securitymatters.utoronto.ca/resources/it-professionals/ - (image)
- https://securitymatters.utoronto.ca/phish-got-a-moment/
- https://unsplash.com/s/photos/email - (image)
- https://unsplash.com/s/photos/castle - (image)
- https://www.sentinelone.com/blog/are-we-done-with-wannacry/
- https://www.kaspersky.com/resource-center/threats/ransomware-wannacry
- https://www.av-test.org/en/
- https://www.forcepoint.com/cyber-edu/heuristic-analysis
- https://www.zdnet.com/article/flashback-trojan-wake-up-call-for-mac-users/
- https://cofense.com/knowledge-center/signs-of-a-phishing-email/
- https://www.pexels.com/photo/man-in-red-shirt-wearing-black-framed-eyeglasses-3965246 – (image)
- https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57pt1r5.pdf
- CISSP: Certified Information Systems Security Professional Study Guide, 6th Edition by Darril Gibson; James M. Stewart; Mike Chapple ; Backups Chapter
- https://www.ssh.com/academy/ssh/protocol

Thank You!
Questions?