
Cybersecurity Awareness for Executives

Cybersecurity Awareness Program

Cybersecurity Services Division
Service Alberta
2022/23



Agenda



Understanding the GoA Cyber Threat Environment



Executives as a Target

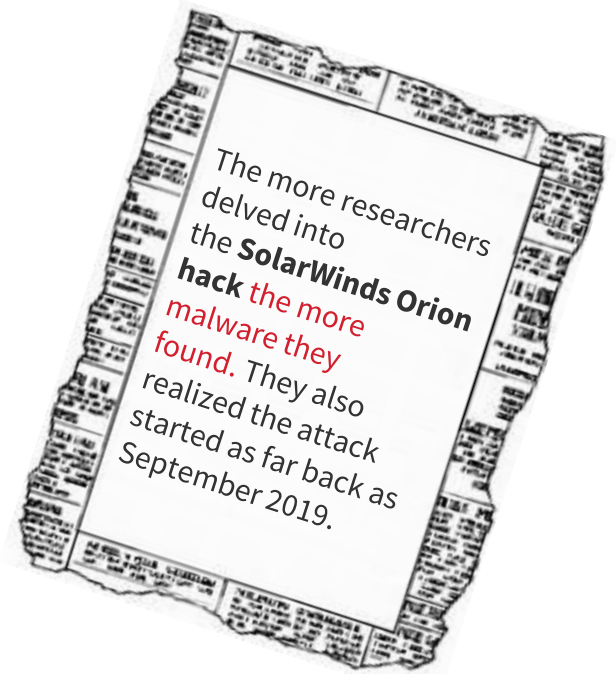
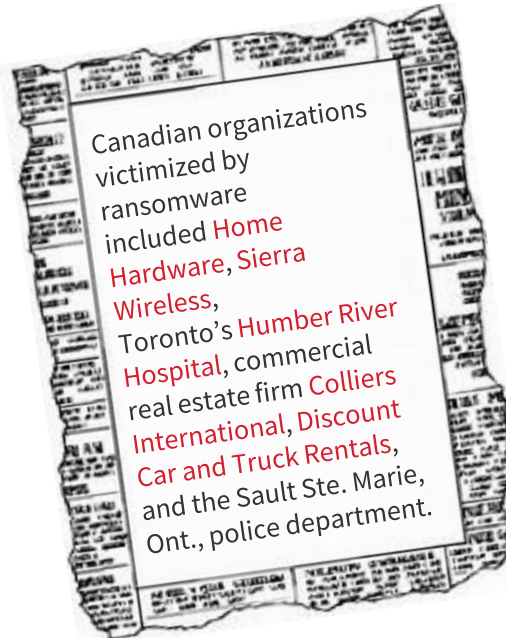
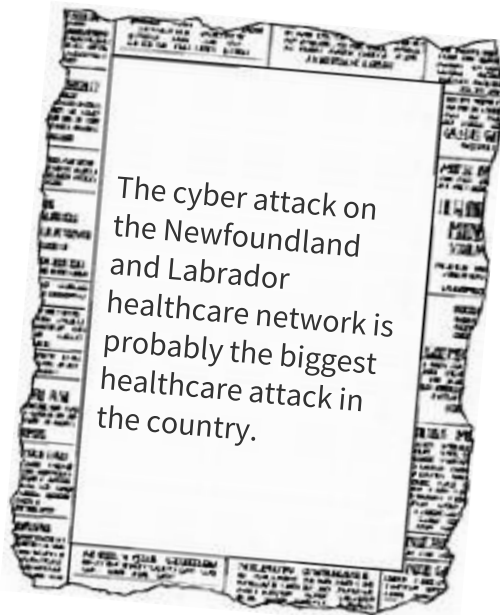


WWYD?

Understanding the GoA Cyber Threat Environment

What are some of the threats that the GoA faces?

Omnipresence of the Cyber Threat



Is the Cyber Threat Real?

Government of Alberta



Unwitty Insider

Systems users' lack of cyber threat awareness often results in accidental loss of data confidentiality, integrity or availability when users either reveal secure information or personal credentials.

GOAL:
None (accidental or due to negligence)

Email phishing to steal digital credentials:

- New phishing prevention tools blocked 2,899 attacks in the first 12 weeks of use

Email, document, or website-based malware:

- Annually, 56% of emails received by GoA are blocked due to identified malicious content
- In 2020-21, 2,918 desktop malware infections were detected and prevented by antivirus controls



Hacktivists

Hacktivists look for confidential information to reveal to the outside world, or perform website defacing or cyber-attacks to disrupt services, thereby impacting the trust relationship between the organization and its clients.

GOAL:
To shame the organization

Network Denial of Service (DoS) attacks:

- Common to entire Canadian public sector
- Since March 2020, between 5 to 30 DoS or scan attacks weekly

Vulnerability scanning:

- 43 million denied GoA network connections per day



Natural Disasters

Natural disasters are random events that cannot be predicted impacting IT services availability (eg: events such as power outages or critical events such as tornadoes or floods.)

GOAL:
None (random)

Critical government systems:

- There are 149 critical systems GoA departments depend on (recovery time objective < 24hrs)

Significant incidents:

- In July 2018, the "impossible" happened when the Agriculture data centre was taken out by a fire, and the Education data centre by a water-main break within 24 hours



Cyber Spies

Often, but not always, sponsored by nation states with competing interests, cyber spies are after trade secrets and other confidential information that could give an edge to a competitor or provide political advantages.

GOAL:
To gain competitive edge

Network scan attacks:

- 157 million denied GoA network connections per day
- 36% from United States



Malicious Insider

Internal users have full access to the data they need to perform their duties. Disgruntled or malicious insiders can find ways to share information with unauthorized parties for profit or for malicious intent.

GOAL:
Make a profit, or shame organization



Terrorists/Nation States

Terrorists are often sponsored by nation states with competing interests. Their attacks aim at disrupting services, causing economic impacts and loss of trust from clients, or sometimes worse, threatening human lives.

GOAL:
To disrupt services and to scare or hurt people



Cyber Criminals

Criminals have found a safe medium to commit crimes anonymously. Crimes include fraud, identity theft, ransomware, and many other activities. Sometimes internal.

GOAL:
To make a profit



Qualified Personnel

The world-wide shortage in cybersecurity professionals has had a major impact on the ability to proactively manage cyber threats versus responding to incidents. Remuneration not currently competitive for qualified staff.

GOAL:
None (risk)

Information breaches continue to be a concern:

- 68 information breaches were investigated in 2020-21
- All breaches were the result of employee actions (accidental or malicious)

Digital Forensic Investigations:

- 104 digital forensic investigations performed in 2020-21 due to confirmed information breaches or misuse of government assets

Network Denial of Service (DoS) attacks:

- Since March 2020, between 5 to 30 DoS or scan attacks weekly

Primary attack vector is email phishing:

- Aug 2020: 12 GoA accounts compromised by an organized Turkey-based group

Foreign network traffic:

- 54% of network traffic comes from outside of Canada

Primary attack vector is social engineering:

- Annually, 56% of emails blocked as malicious
- May 2021: spear phishing attack on 204 users, 3 purchased gift cards as instructed by attacker (monitoring stopped cards transfers)

Cybersecurity related incidents:

- 258 of the 563 incidents in 2020-21 were due to malicious actors' actions

Ransomware:

- 3 Alberta schools and 2 public agencies impacted in past 5 years, all paid ransoms

World-wide shortage in cybersecurity resources:

- Conservative estimate of 1.8 million gap in qualified cybersecurity personnel by 2022

Attracting and retaining qualified personnel:

- Lost 19 cybersecurity staff since Jan 2019
- Cybersecurity Services have not reached full complement of 43 filled positions since Jan 2019, impacting projects and proactive threats management

Executives as a Target

Why are we here to talk to you?

Why are Executives a Target?

- From an attacker's perspective, **an executive is the highest-value target** to hunt as they:
 1. are privy to the most important and confidential data and business processes
 2. often have application access privileges far greater than those granted to lower-level employees
 3. may have access/control over their organization's finances
 4. tend to be lax about following security procedures

WWYD?

What would you do?



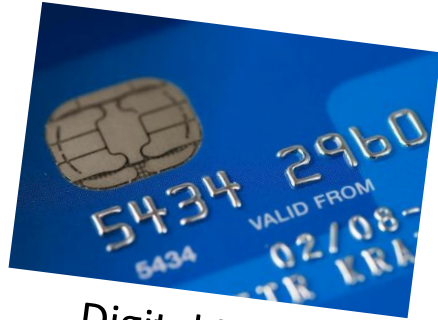
Travel



Shadow IT



Least Privilege



Digital Fraud



Phishing



Risk Management



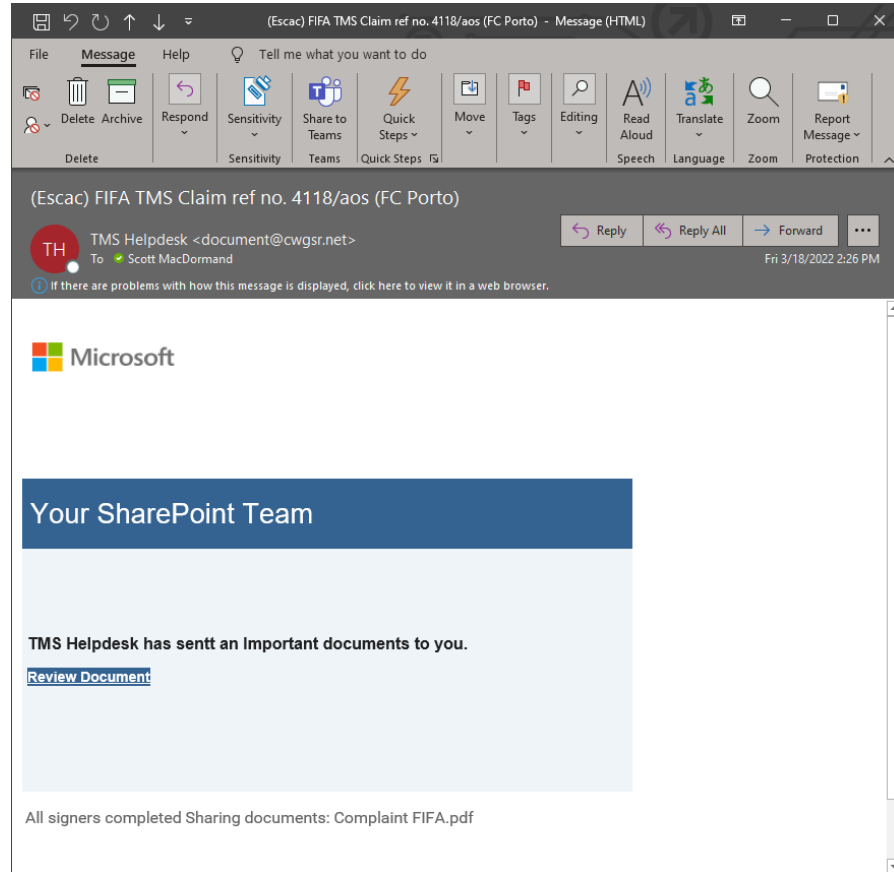
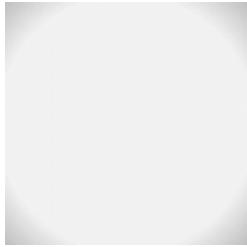
Phishing

Phishing and other related attacks

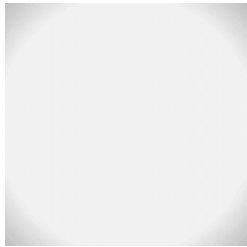
- Indications of phishing
 - Misspellings (becoming less common)
 - Account status threats
 - Requests for personal information
 - Fake domain names/links
 - Spoofed email address
 - Sense of urgency
- Other types of phishing
 - Spear Phishing and Whaling
 - SMShing and Vishing
 - Quid Pro Quo



Example Phish #1



Example Phish #2



ACTION REQUIRED: Please review the completed documents - Message (HTML)

File Message Help Tell me what you want to do

Delete Archive Respond Sensitivity Share to Teams Quick Steps Move Tags Editing Read Aloud Translate Zoom Report Message

Delete Sensitivity Teams Quick Steps Speech Language Zoom Protection

ACTION REQUIRED: Please review the completed documents

EM Emma Michael <emma.michael@gov.ab.ca>
To Scott MacDormand

Reply Reply All Forward


Fri 3/18/2022 2:36 PM


Hello Scott MacDormand,

Procurement Services has recently switched to DocuSign for Government of Alberta contracts.

We ask that you please review the following document for correctness.

DocuSign



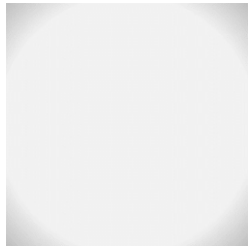


Your document has been completed.

[VIEW COMPLETED DOCUMENTS](#)

Emma Michael
Procurement Specialist
Tel: (780) 124-5647

Example Phish #3



The screenshot shows an Outlook window titled "Re: COVID-19 (Payroll Adjustment) - Message (HTML)". The ribbon includes "File", "Message", and "Help". The "Message" ribbon has buttons for "Delete", "Archive", "Respond", "Sensitivity", "Share to Teams", "Quick Steps", "Move", "Tags", "Editing", "Read Aloud", "Translate", "Zoom", and "Report Message".

The email header shows the subject "Re: COVID-19 (Payroll Adjustment)", the sender "Chris Lawther <ChrisLawther@GBMC.ac.uk>", and the recipient "To Scott MacDormand". The date and time are "Fri 3/18/2022 2:42 PM".

The body of the email contains the following text:

All staff & employee of are expected to verify their email account for new payroll directory and adjustment for this month benefit payment. Please kindly Click

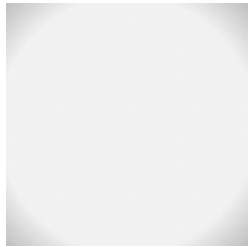
[CURRENT MONTH-BENEFIT](#)

and complete the required directive to avoid omission of your benefit payment for this month.

Thank you,

Payroll Admin Department.

Example Phish #4




Ellen Paulwood shared "Meeting 2021- Agenda DRAFT" with you.

Ellen Paulwood <notify@yourbestdefense.com>
To: Scott MacDormand


Fri 3/18/2022 2:48 PM


EXTERNAL



Ellen Paulwood shared a file with you

"Hi, please refer to the documents all paid No. 10."

 Meeting 2021- Agenda DRAFT

 This link will work for Scott.Macdormand@gov.ab.ca

Open

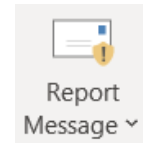
Microsoft Privacy Statement

Phishing Giveaways

- ‘Reply’ to the message to see if it was spoofed
 - Does john.doe@gov.ab.ca become fooledyou@tricky.phish.ru ?
- Do the links in the message look suspicious?
 - Hover your mouse over the link to see if it looks legitimate
- Are there unexpected attachments or attachments that you don’t normally get?
 - **Don’t open the attachments, as they may contain malware!**

Take Preventive Action

- Call or email the person or organization using their legitimate information to verify the request
 - Don't assume that any message is necessarily legitimate!
- DELETE suspicious messages
 - Use the **Report Message** button in Outlook
- Contact financial institutions you deal with to verify requests



Don't be a Victim!

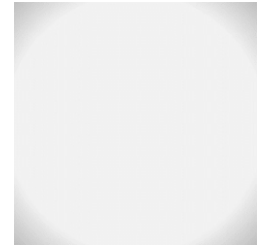
- Change the password on any accounts that you may have divulged credentials
- Contact financial institutions you deal with immediately to have any fraudulent changes reversed or cancelled
 - Put a hold on accounts if possible
- Contact the GoA Service Desk and have them create an incident ticket
- Continue to monitor any affected account(s) or systems for unusual or fraudulent activity



Travel

Example: Cruising Southeast Asia

- You are planning a cruise of Southeast Asia, which includes stops in China, Vietnam, Thailand, Cambodia, Malaysia, and Singapore
- You want to bring your GoA cellphone and/or laptop with you to stay in contact with family and work
- Is this a good idea and what would you do?



Travelling as an Executive

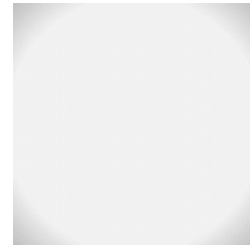
- When executives travel to foreign countries, they can become targets for foreign governments or other malicious actors
 - **need to take extra precautions when traveling with corporate-owned devices**
 - assume that your communications are (perhaps actively) monitored
 - best to consult with Cybersecurity Services and/or Provincial Security & Intelligence Office (PSIO) before travelling
 - PSIO-security@gov.ab.ca



Least Privilege

Example: ARTS Access

- An ARTS administrator from your department transfers to a new ministry
- After the transfer, it is discovered that they still have access to your ministry's requests
- What would you do?



Least Privilege

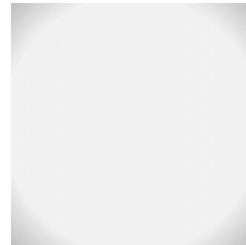
- **Privilege creep** is caused when users are granted (information) access privileges for their role, but they are not immediately removed when the person changes roles or leaves the organization
- **Least privilege** means a user is given the **minimum** amount of access required
- Executive (and their assistant/staff) positions and roles typically allow a great deal of access
 - **Access should be reviewed on a regular basis!**



Digital Fraud

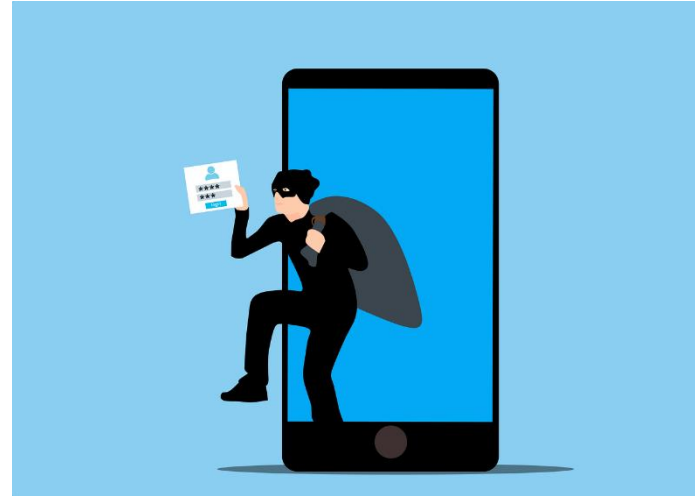
Example: Send Money Fast!

- You or your EA receive an email that appears to be from your DM, minister, or even the Premier
- The email is asking for you to immediately transfer funds to one of the vendors that you deal with so that support doesn't get cancelled
- The email seems legitimate and has a sense of urgency
- What would you do?



Many types of Digital Fraud

- Charity fraud
- Internet ticket fraud
- Online gift card fraud
- Social media fraud
- Purchase fraud
- Advance-fee fraud



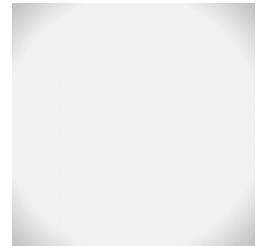
**Verify with the sender if
the message is legitimate!**



Shadow IT

Example: Purchasing IT Services

- One of your business area wants to use a SaaS product that allows them to easily manage a project they are working on with external agencies, including storing project documentation
- They purchase several licences using a Pcard
- Nobody in IMT is informed of this purchase
- Is this an ok software purchase?



Shadow IT Risks

- Lost control and visibility
- Lost data
- Cost control



Service Alberta should be your point of contact for IT projects and resources!



Cloud SaaS Risks

- GoA Cloud Enablement Program should be first point of contact for any cloud-based solution/service
 - <https://modernization.sp.gov.ab.ca/CloudProgram/SitePages/Home.aspx>
 - <https://abgov.sharepoint.com/sites/S500D20-CTS/SitePages/Cloud-Computing---Information-%26-Training.aspx>
- Can also work with Cybersecurity Services to assess the risk of using the solution/service
 - Reminder: If the solution/service is free, you are the product!

Cyber Risk Management

How can I address cyber risk in the GoA?

- Have your staff completed mandatory cybersecurity awareness courses in Noverant?
 - Includes information on phishing
- Have you recently reviewed the access to the information under your department's control?
 - this would include applications as well as shared network drives, SharePoint, and OneDrive
- Have you reviewed your business processes to look for risks or where fraud could occur?
 - Helps with insider threats

How can I address cyber risk in the GoA?

- Is your area using shadow IT instead of enterprise solutions?
 - may be putting GoA information at risk
- Does your business area have a method to track cyber risk?
 - Cybersecurity Services is responsible for tracking IMT risk

What is my Role for Cybersecurity?

- GoA policies speak to Department Heads as being accountable for ensuring compliance to all GoA Information Security Policy Instruments
 - IMT Policy Instruments site:
<https://imtpolicy.sp.alberta.ca/SitePages/Home.aspx>
 - this includes addressing information security risk in their department
 - responsibility is usually delegated down to the ADM or ED level

Technologies to Address Risk

- The DM of Service Alberta is accountable for Information Security controls, standards, processes, and compliance implemented across the GoA
- Service Alberta has deployed technologies that help protect the GoA environment and manage information security risks
 - block almost all SPAM and phishing emails
 - block access to known malicious web sites that have a reputation for supporting phishing attacks or hosting malware
 - antivirus and malware detection on GoA desktops and laptops
 - controls that prevent easy sharing of Protected C information

Cybersecurity Services and Risk

- Cybersecurity Services also works with departments to perform risk assessments on their applications and on how their data is being protected
 - Advise/collaborate with business areas on cyber and application risk mitigation
 - Track IMT risk across the GoA environment

Questions?

Cybersecurity Services Division
cybersecurity@gov.ab.ca

