Multi-Factor Authentication

Province of BC's Journey to onboarding MFA and moving towards Zero Trust

BRITISH COLUMBIA | Ministry of Citizens' Services

Agenda

- Introduction: Who are we?
- Story time: Understanding an attacker.
- What is MFA and how is the Province of BC supporting its adoption.
- How MFA is used in your daily life.
- What is Zero Trust and how is the Province of BC supporting its adoption.
- Scope of the Province's MFA project.
- What's next for MFA?
- Sharing some lessons learned.
- Questions.

Introduction: Who are we?

- Jesse Piccin:
OCIO/ISB's Director for ADMS:
Access and Directory Management Services

- Dale Land:
OCIO/ISB's Director Cyber Intelligence
and Investigations

OCIO | OCIO CIRMO | OCIO DPD | OCIO ES | SBC | GDX | RPD

Story time: Understanding an Attacker

- Likes to use **Phishing** attempts to steal credentials by tricking users to log into a spoofed website that looks real.

- May use **brute force attack:** In cryptography, a brute-force attack consists of an attacker submitting many passwords or passphrases with the hope of eventually guessing correctly. The attacker systematically checks all possible passwords and passphrases until the correct one is found.

- **Password stealing malware** can be used to download a variety of threats onto compromised machines to then steal sensitive information, including usernames and passwords.
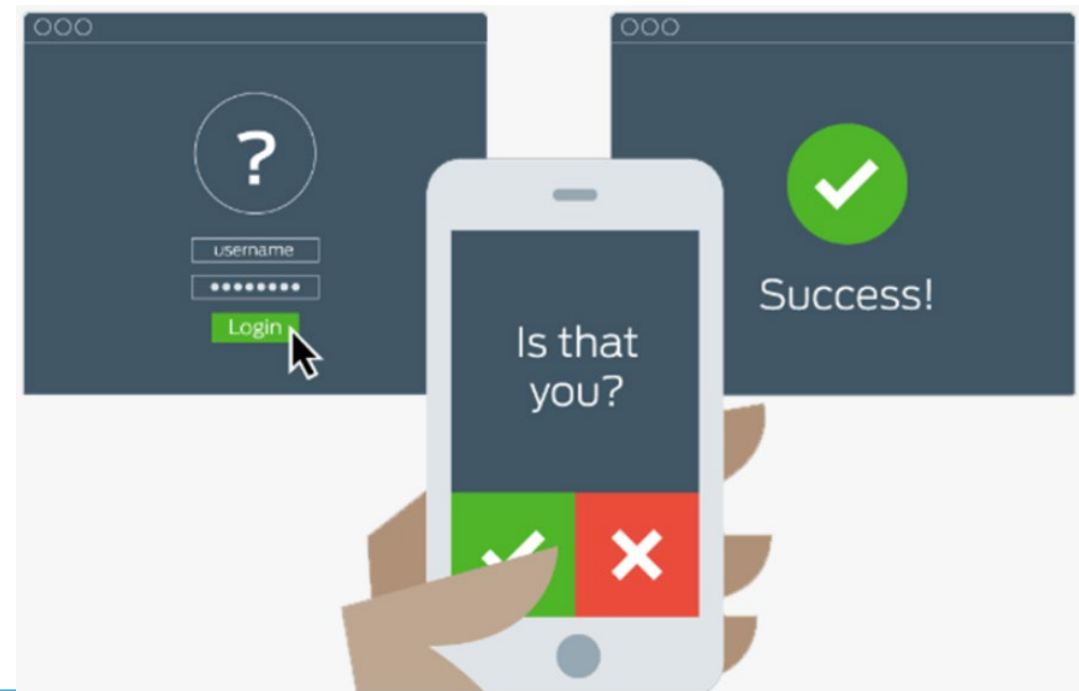
How can we help prevent an attacker from being successful?

Use MFA!

Microsoft says that *"users who enable multi-factor authentication (**MFA**) for their accounts will end up blocking 99.9% of automated **attacks**"*

OCIO ES   SBC   GDX   RPD   PSD   CSD

Multi-Factor Authentication provides a higher assurance that the correct person is appropriately accessing services and applications.

What is MFA?

PASSWORD

VERIFICATION

ACCESS

LOGIN REQUEST

SUCCESSFUL LOG IN

1ST FACTOR + **2ND FACTOR** =

Typical MFA Factors:

1st factor is *"What You **Know"*** IDIR ID & Password **(current state).**

2nd factor is *"What You **Have"*** Smartphone with MS Authenticator app, Call Back number or Token **(Future state).**

MFA is used in your daily life: At home and at play!

How is the Province of BC embracing MFA?

Apply MFA where it's needed most

1) Start with enabling MFA for the Province's Azure Cloud based services (MS Teams, Exchange Online, OneDrive, etc)

2) Enable MFA for VPN, DTS/Citrix Services and Azure Active Directory SaaS based integrations.

OCIO

OCIO CIRMO

OCIO DPD

OCIO ES

SBC

GDX

RPD

PSD

OCSD

Embrace Zero Trust principles

What else is needed besides MFA?

Verify explicitly

Always authenticate and authorize based on all available data points, including user identity, location, device health, service or workload, data classification, and anomalies.

Use least privileged access

Limit user access with just-in-time and just-enough-access (JIT/JEA), risk-based adaptive polices, and data protection to help secure both data and productivity.

Assume breach

Minimize blast radius and segment access. Verify end-to-end encryption and use analytics to get visibility, drive threat detection, and improve defenses.

OCIO

OCIO CIRMO

OCIO DPD

OCIO ES

SBC

GDX

RPD

PSD

OCSD

Some of the Province's Zero Trust planned initiatives

What else is needed besides MFA?

- PIM (Privileged Identity Management)
- PAM (Privileged Access Management)
- PAW (Privileged Access Workstations)
- Azure Risk Based Policies
- Azure Defender for Identities
- Azure Defender for Endpoints
- Plus more!

OCIO

OCIO CIRMO

OCIO DPD

OCIO ES

How secure is your password?

TIME IT TAKES A HACKER TO BRUTE FORCE YOUR PASSWORD

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	1 sec	5 secs
7	Instantly	Instantly	25 secs	1 min	6 mins
8	Instantly	5 secs	22 mins	1 hour	8 hours
9	Instantly	2 mins	19 hours	3 days	3 weeks
10	Instantly	58 mins	1 month	7 months	5 years
11	2 secs	1 day	5 years	41 years	400 years
12	25 secs	3 weeks	300 years	2k years	34k years
13	4 mins	1 year	16k years	100k years	2m years
14	41 mins	51 years	800k years	9m years	200m years
15	6 hours	1k years	43m years	600m years	15 bn years
16	2 days	34k years	2bn years	37bn years	1tn years
17	4 weeks	800k years	100bn years	2tn years	93tn years
18	9 months	23m years	6tn years	100 tn years	7qd years

HIVE SYSTEMS

-Data sourced from HowSecureismyPassword.net

OCIO   OCIO CIRMO   OCIO DPD   OCI... ES...

Scope of the Province's MFA Project

1

Enable IDIR and Azure Guest users with the ability to respond to **Azure MFA prompt(s)** when accessing **Azure Services, VPN, DTS and SaaS based Azure AD integrations.**

2

Register **40,000+** IDIR users across all Ministries with MFA

OCIO   OCIO CIRMO   OCIO DPD   OCIO ES   SBC   GDX   RPD   PSD   CSD

Recap of the Province's MFA Journey to date

- Originally started out with 4 Cohorts earlier this year, but increased to 6 until end of March 2022.

- Over **60,000+ MFA related emails sent** (MFA self registration emails, reminders, etc).

- Over **100+ MFA outreach events (includes multiple weekly Cohort support sessions, etc)**

- Delivered over **28+ MFA presentations across government**.

- "Too many to count" updates to MFA website, MFA documentation, automated and support scripts, etc.

Successfully registered over 26,000+ BC Public Service Employees with MFA!

OCIO · OCIO CIRMO · OCIO DPD · OCIO ES · SBC · GDX · RPD · PSD · CSD

What's next for MFA?

Over the next few months:

- Complete the majority of MFA registrations for all 40,000+ IDIR users across Government plus Azure Guest accounts.
- Enable MFA for VPN and DTS related services.
- Roll out further security enhancements to our MFA Conditional Access policies.

2022

- Implement additional Zero Trust Azure services (Risk Based Policies, PIM, Defender for Identities and Endpoints, etc).
- Continuously improve upon the new MFA service (Further education/outreach, process improvements, etc).

OCIO | OCIO CIRMO | OCIO DPD | OCIO ES | SBC | GDX | RPD | PSD | CSD

Some MFA lessons learned

- Embracing Cloud Services can save an organization a lot of money…… but securing the cloud is expensive.

- Adopting MFA can be challenging for some users.

- Tricky balancing security needs against "MFA user exhaustion".

- Cloud services are heavily interconnected. Be very careful and cautious when implementing changes.

- A wide variety of cloud security expertise is needed to fully support and maintain the full spectrum of cloud security services that are needed to secure your services and data.

Questions?

Email Jesse.Piccin@gov.bc.ca or IMS@gov.bc.ca

Thank you!

ISB MFA Website

OCIO

OCIO
CIRMO

PSD

CSD