ICI INVESTMENT COMPANY INSTITUTE® ICI Global

# INVESTMENT FUNDS INSTITUTE OF CANADA

Cybersecurity Musings

March 2024

# Agenda

1. Passwords
2. Artificial Intelligence
3. Phishing
4. Threat Intelligence
5. Survey Results

# 2023 Top 20 Most Common Passwords

1. Password
2. 123456
3. 123456789
4. Guest
5. Qwerty
6. 12345678
7. 111111
8. 12345
9. Col123456
10. 123123
11. 1234567
12. 1234
13. 1234567890
14. 000000
15. 555555
16. 666666
17. 123321
18. 654321
19. 7777777
20. 123

# Password Security

- Old Conventions
- Authoritative Guidelines
- Entropy
- Administration

# Password Security – Old Conventions

- Four, Six, or Eight, Character Passwords
- No Requirements
- Password Re-use
- Sequential Passwords
- Exclamation Point at the end of a Password
- E to 3, o to 0, B to 8, etc.
- Digits at the End
- Publicly Available Data

# Authoritative Guidelines

- National Institute of Standards & Technology – 800-63
- National Cyber Security Center
- International Organization for Standardization – 27001
- Many Technology Companies, Vendors, etc.

# Entropy

- A measurement for how unpredictable is a password
- $\mathrm{E} = \log 2\,(R^L)$
  - E = Password Entropy
  - R = Pool of Unique Characters
  - L = Number of Characters in your Password
  - $R^L$= Number of Possible Passwords
  - $\mathrm{E} = \log 2\,(R^L)$ = The Number of Bits of Entropy
- So, an 8 character password (in English) in all lowercase is $26^8$ or 208,827,064,576 possible combinations.
- Computers work in binary so that is roughly $2^{38}$ or 38 bits of Entropy.
- Today many passwords are $72^8$ or $2^{49}$ or 49 bits of Entropy.

# Administration

- Rotate passwords every 90 days – NO!
- Require complex passwords – NO!
- Multifactor Authentication is bullet proof – NO!
- Biometric access is fail safe – NO!
- Administrators/Software Developers should follow policy – YES!

# Artificial Intelligence

- Generative AI – ChatGPT
- WormGPT
- Voices and Images
- Hands and Numbers
- Prompt Training
- **Risks:**
  - Transparency
  - Privacy
  - Security
  - Trust
  - Ethics

**Benefits:**
Efficiency
Productivity
Speed
Quality
Services

# Phishing

- Top Vector of Attacks
- Social Engineering: Voice, Text, Social Media, Images
- Administrative Assistants
- Compromised Credentials
- Facebook & Google Scam - $100 Million
- Not Petya - $10 Billion+
- Ukrainian Power Grid
- Ubiquity - $50 Million
- FACC - $50 Million

# Threat Intelligence

- Which Threat?
- Definition: In both the public and private sector, intelligence is the end-product of a structured process that collects and processes information to glean insights*.
- Strategy: Priorities, staff, sources, share.
- Sector Threat Intelligence Program.
- What defines success?

* Rebel Global Security