CYBERSECURITY 101

Vigilant
Sceptical
Safe

Réjean Gravel
Chief Information Officer and
Director General of Information and Technologies,
Environment Canada (retired)

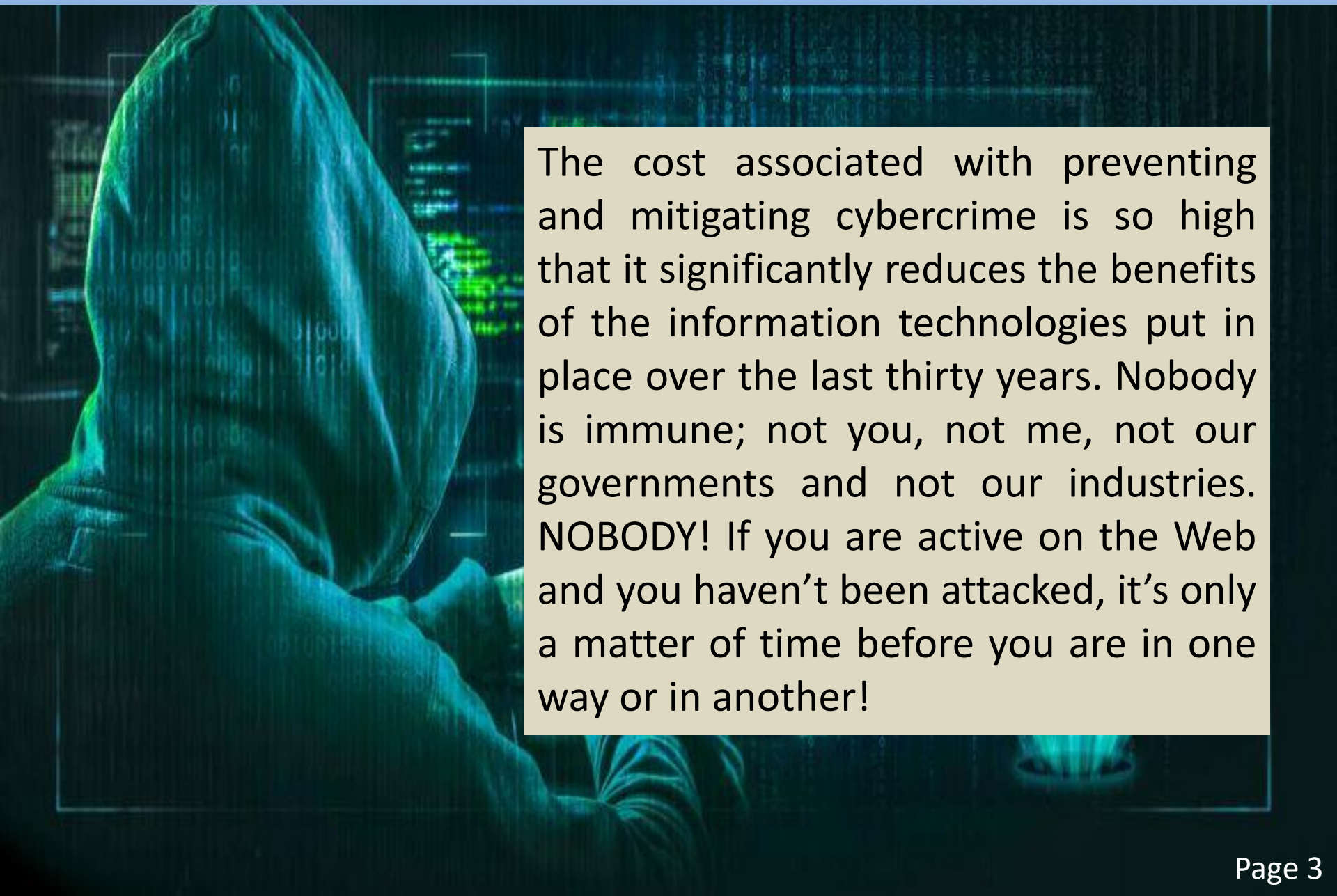
March 9, 2022

Presented to the Canadian Club Canadien Gulf Coast Florida

WHAT I WILL TALK ABOUT TODAY

1: Context
2: Consequences of cybercrime
3: Attacker profiles and motivations
4: The business of cybercrime
5: Good practices
6: What to do if you get hacked
7: Conclusion

1: CONTEXT

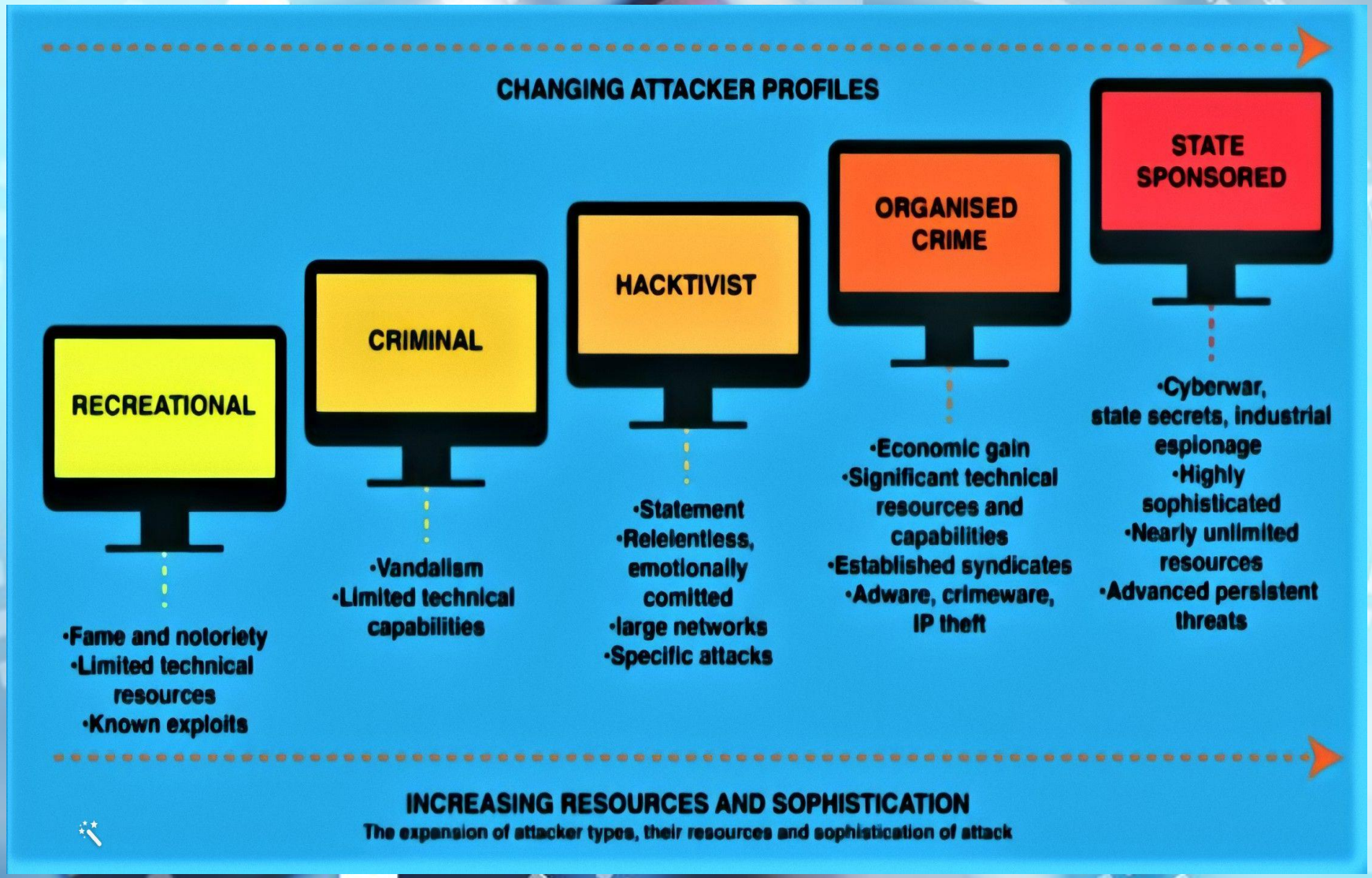


The cost associated with preventing and mitigating cybercrime is so high that it significantly reduces the benefits of the information technologies put in place over the last thirty years. Nobody is immune; not you, not me, not our governments and not our industries. NOBODY! If you are active on the Web and you haven't been attacked, it's only a matter of time before you are in one way or in another!

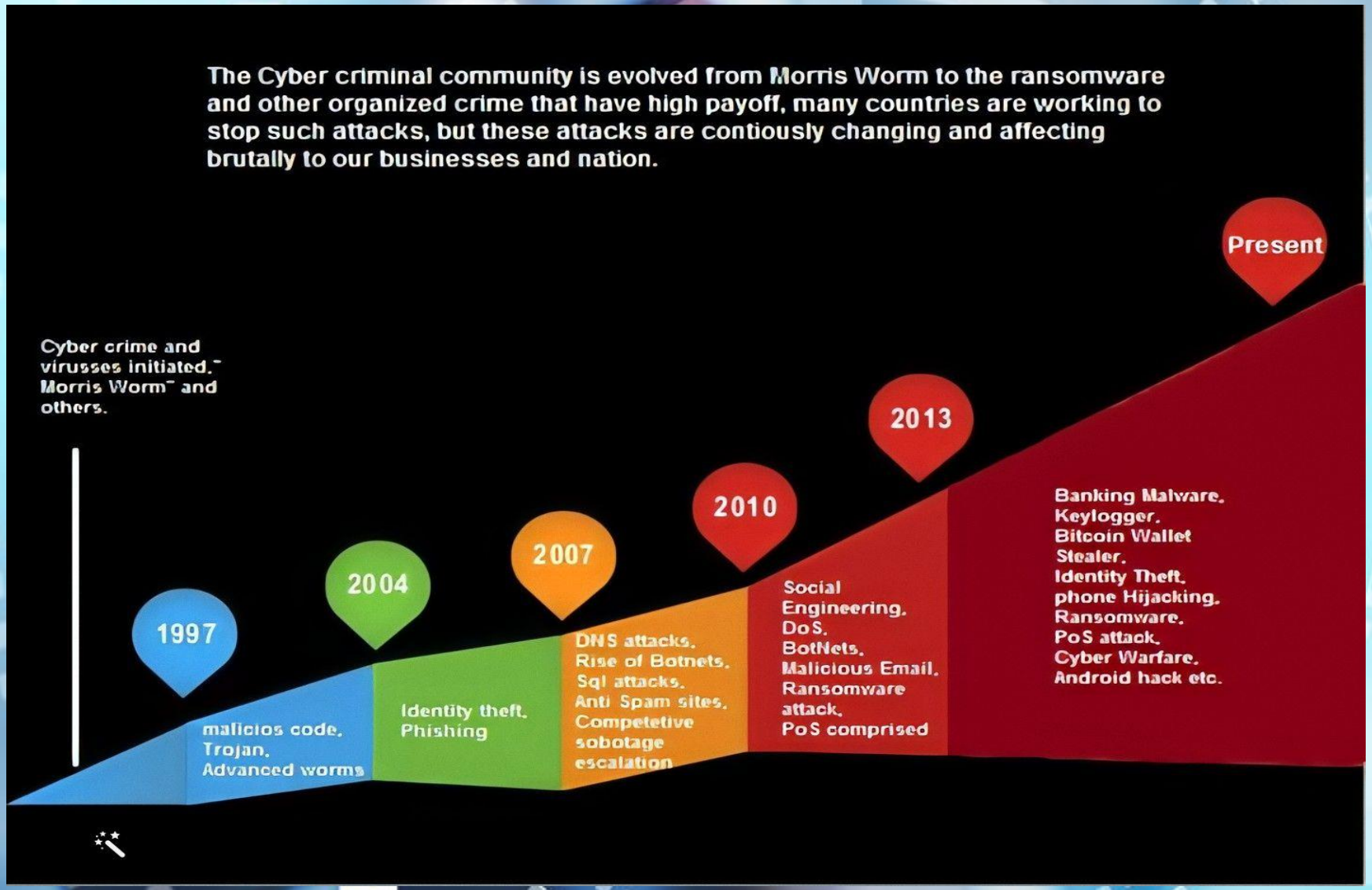
2: CONSEQUENCES OF CYBERCRIMES

FOR WHO	SOME POTENTIAL NEGATIVE CONSEQUENCES
INDIVIDUALS	Financial loss; impact on reputation and career; divulging or wrongful use of information with direct impact on personal life; identity theft; stress; sickness; suicide.
COMMERCES, ENTREPRIZES AND INDUSTRIES	Production or service downtime; financial loss; client base loss; impact on reputation; legal action; loss of corporate secrets; loss of competitiveness due to the divulgation or wrongful use of corporate information; bankruptcy.
ESSENTIAL INFRASTRUCTURES	Interruption of essential services (ex: water services) impacting the health, wellness, and the physical and financial security of citizens; significant economic impacts; loss of confidence; loss of client base.
GOUVERNMENTS	Impacts on the health, wellness, and the physical and financial security, impact on services to citizens; biased policies; loss of confidence in governments; uprising; violence; tense diplomatic relations; war.

3. ATTACKER PROFILES AND MOTIVATIONS



4. THE BUSINESS OF CYBERCRIME

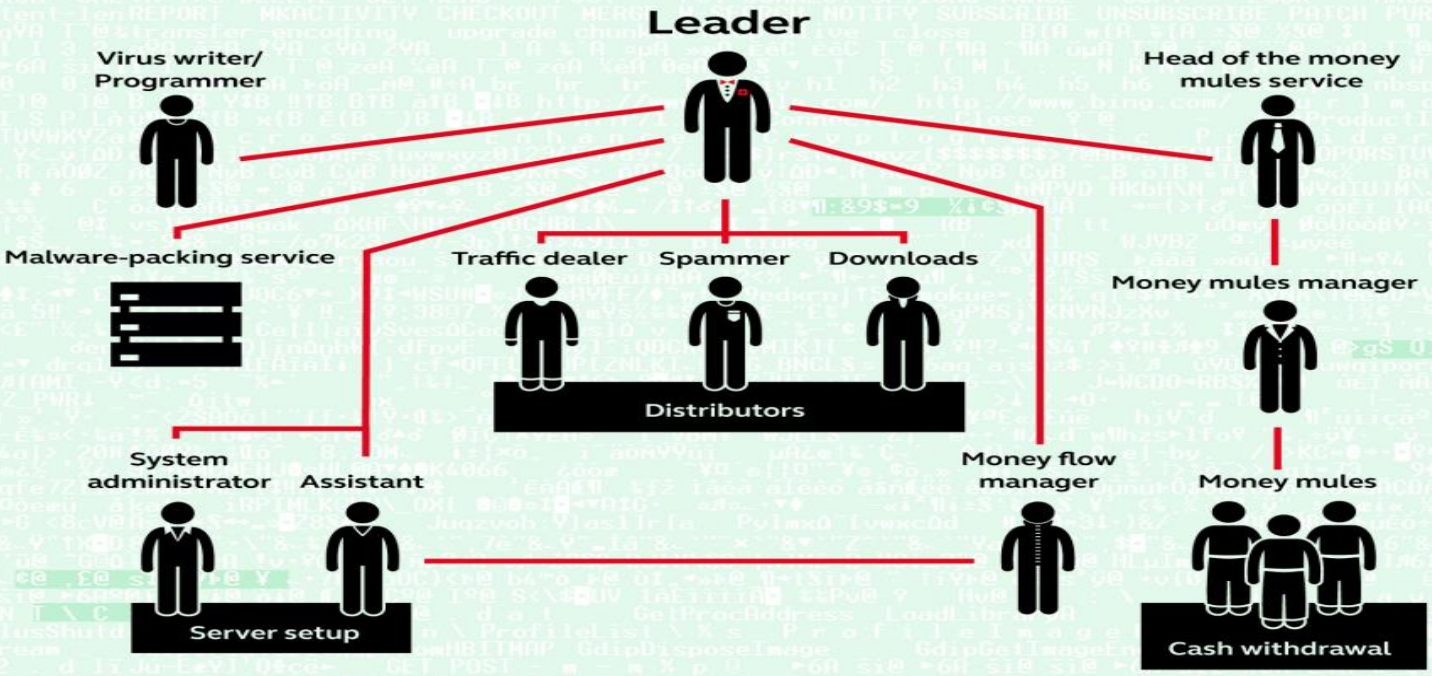


4. THE BUSINESS OF CYBERCRIME (CONT'D)

4. THE BUSINESS OF CYBERCRIME

How a financial cybercrime group is organized

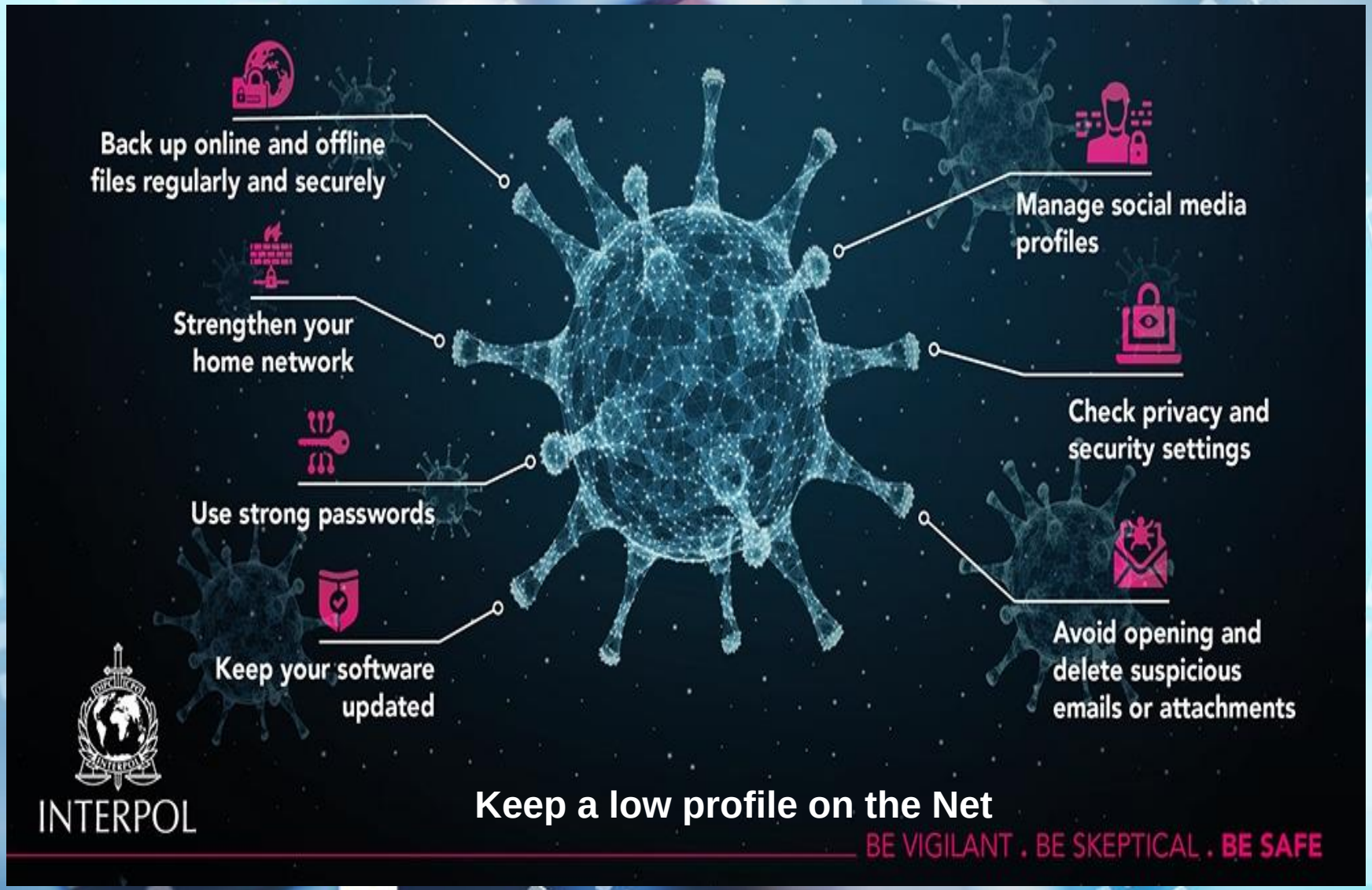
Kaspersky Lab is actively investigating five large, Russian-speaking cybercriminal groups involved in stealing money using malicious software.



The Money flow manager transfers funds from attacked financial accounts to accounts provided by the Money mules manager. The Money mules manager instructs the money mules where to transfer the money. A share of the stolen money ends up with the Head of the money mules service, while the rest is transferred to the Leader of the criminal group.

KASPERSKY

5. CYBERSECURITY GOOD PRACTICES



5. CYBERSECURITY GOOD PRACTICES (CONT'D)

- ✓ Choose a browser that protects your privacy and collects a minimum of data on you. Google is the worst!
- ✓ Avoid social media like Facebook and Instagram.
- ✓ Manage security and privacy settings.
- ✓ Use two-factor authentification wherever you can, especially for online banking.
- ✓ Use long, complex passwords using capital letters, numbers, and symbols such as Ugo&7100rg50!
- ✓ Do not use the same password everywhere.
- ✓ Change your most important passwords (i.e. banking and online shopping) every few months.
- ✓ Apple devices are more secure but not perfect.
- ✓ Virtual Private Networks (VPN) will hide your information and encrypt your personal data for your privacy and protection.

5. CYBERSECURITY GOOD PRACTICES (CONT'D)

- ✓ Good anti-virus & malware software like Norton will help.
- ✓ Do not open suspicious emails – delete them immediately.
- ✓ Do not store passwords on your browser. It's convenient but easy to access for hackers.
- ✓ Do not store your password list on your desktop! ☹☹☹
- ✓ Keep your computer and iPhone updated – updates contain patches to address vulnerabilities.
- ✓ Back-up your data. Cloud storage services like Dropbox are convenient ($), but you can back up on a large USB key(free).
- ✓ Subscribe to identity protection services like Equifax (not the best but OK). Your bank may offer a much better one.
- ✓ Have a second laptop/phone that you can use while your main one is infected.
- ✓ Do not use public unsecured wi-fi, especially abroad!

5. CYBERSECURITY GOOD PRACTICES (CONT'D)

- ✓ If you do not recognize the phone number, and it is only made of numbers, do not answer!
- ✓ Emails or phone call saying: you have a parcel at customs, the RCMP is after you, you won someting – these are scams.
- ✓ If you are subject of a ransomware attack, consider paying the amount unless you have good backups and are willing to rebuild you laptop.
- ✓ Jokes emails might be fun, but they are often a source of viruses and malware. Beware!
- ✓ Chain letter emails are scams called socio-engineering. They are designed to slow down the internet – they may also contain viruses. Do not forward to anybody.
- ✓ Do not visit illicit websites just to check. You might regret it.
- ✓ If it's too good to be true; it's not true!

5. CYBERSECURITY GOOD PRACTICES (CONT'D)

- ✓ Once you find the website you are looking for using Google or another search engine, check the address bar at the top of the screen and look for HTTPS and not HTTP. The S means secure website. All serious business now use HTTPS.
- ✓ Hackers sometimes use the email name of someone you know to hide their identity (it's called spoofing). Before you open the email, you can place your cursor over the name to ensure it is the person you know and not someone "spoofing" you.
- ✓ Microsoft Windows: the least secure but getting better.
- ✓ Apple IOS: very secure and widely available, but costly.
- ✓ Google Android: competes with IOS, cheaper, less secure.
- ✓ Linux Based Ubuntu: fast, secure, inexpensive and stylish operating system. You can buy a laptop with Ubuntu or upgrade yours if you are good with laptop technology.

6. WHAT TO DO IF YOU GET HACKED

It all depends on the type of attack. Having your Facebook hacked is one thing, having your bank account hacked is something else. The following is a list of actions that you might have to take.

- ✓ Change all your passwords, especially if you used the hacked password on other websites, using secure password.
- ✓ Call the companies involved (ex: Facebook) and ask for help.
- ✓ Check your bank account and credit cards - call your bank(s).
- ✓ Tell your family and friends, you have been hacked.
- ✓ You may need a new email account.
- ✓ You may need your hard disk to be wiped out and rebuilt from scratch – Windows, MS Office, and every application and software you had (use a professional service to do that).
- ✓ Implement the measures identified in Section 5.

7. CONCLUSION

INFORMATION AND TECHNOLOGIES CHANGED THE WORLD WE LIVE IN IN COUNTLESS POSITIVE WAYS. UNFORTUNATELY, EVERY TECHNOLOGY HAS A DARK SIDE. CYBERCRIMINALITY IS A THRIVING BUSINESS AND A NEW CLASS OF WEAPONS OF MASS DESTRUCTION. WE HAVE BEEN TOO NAIVE AND LENIENT. WE MUST TAKE DRASTIC MEASURES AT ALL LEVELS TO CONTROL AND REDUCE THE NEGATIVE IMPACT OF CYBERCRIMINALITY.

IT STARTS WITH YOU AND ME!

CYBERSECURITY 101

Vigilant
Sceptical
Safe

Réjean Gravel

Chief Information Officer and
Director General of Information and Technologies,
Environment Canada (retired)

March 9, 2022

Presented to the Canadian Club Canadien Gulf Coast Florida