ONLINE SECURITY

FrenchMarketing.ca Review Document

Managing Security Risks

Thomas Hormaza
French Marketing

Part 1 | What is Online Security?

Online Security Defined

"Computer security, cybersecurity or information technology security (IT security) is the protection of computer systems from the theft of or damage to their hardware, software, or electronic data, as well as from the disruption or misdirection of the services they provide" - Wikipedia

Part 2 | Why is it Important for your Business?

Online Security and your Business

Avoiding Damage to your Reputation as well as lost revenue and lost productivity!

Statistics Canada 2017:

21% of **Canadian businesses were impacted** by cyber security incidents

54% of those businesses reported the incidents **prevented employees from carrying out work**

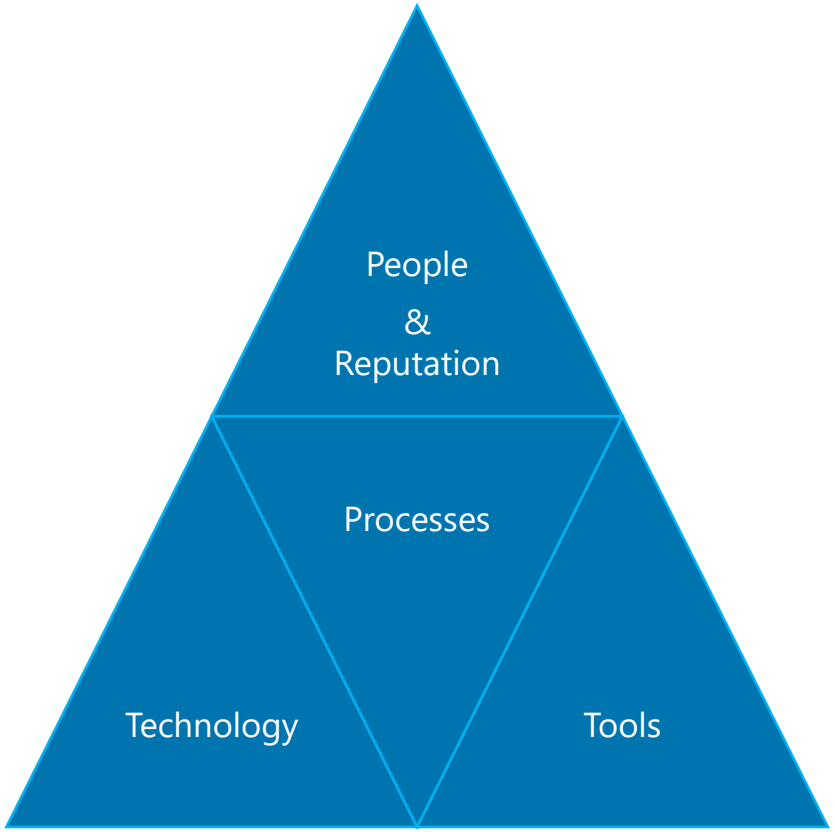
10% of businesses in Canada reported that they **lost revenue**

6% businesses reported that the **incidents damaged the reputation** of their business

https://www150.statcan.gc.ca

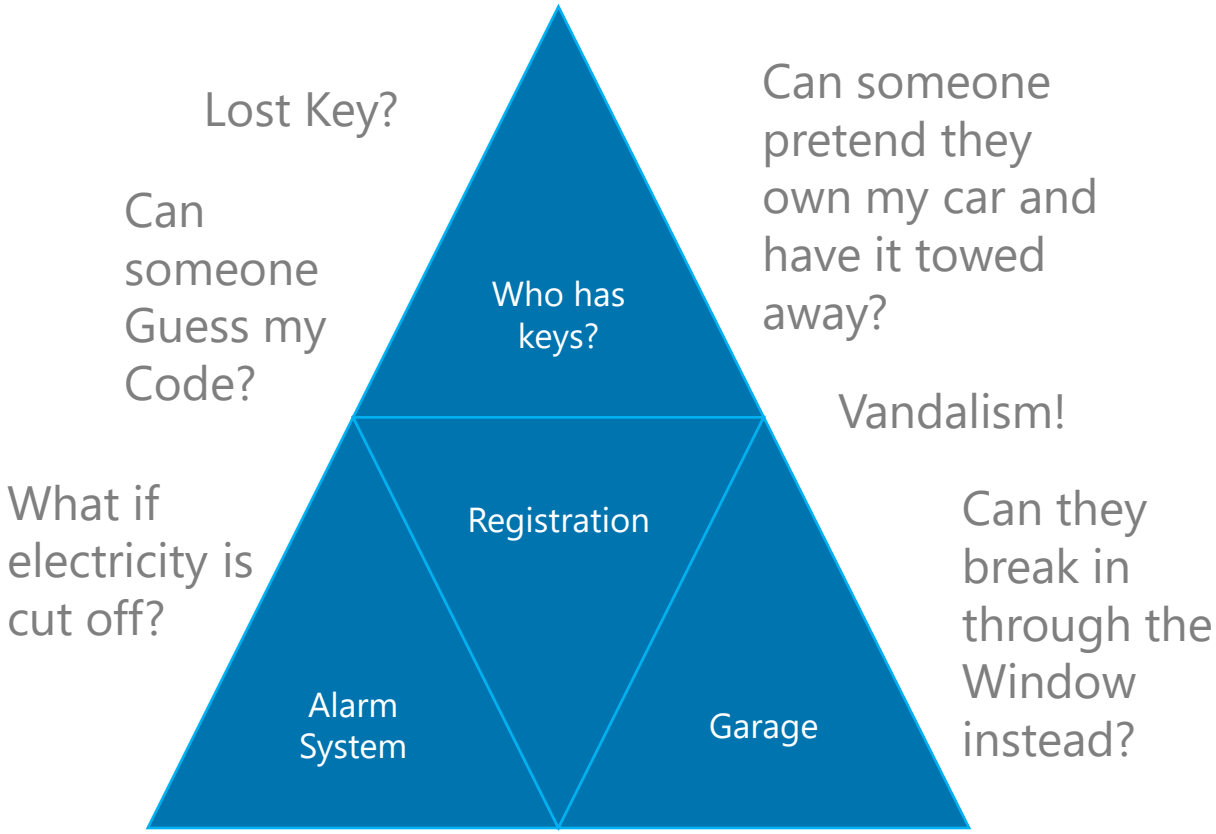
Thinking like a Hacker to Improve your Security

Your Business is an Asset!



Is my Business at Risk?

But what if it was your Car?



Think of other examples

People, Passwords, Devices and Communications

Use **Passwords that are VERY difficult to Guess** (12 characters with symbols, numbers, up/lower cap)

Do not Share your Password with others and **Do not Share Accounts** with others (Email, Work Facebook Channel, Supplier Account Access, Shopify, Amazon)

Do not let others use your devices (PC, Phone, Voicemail, Tablet, USB Key) and **don't lose them!**

Store Devices in a Safe Location (PC, Phone, Voicemail, Tablet, Backup Drives, USB Key)

Part 4 | What you Can Do - People

People, Passwords, Devices and Communications

Do not click before reading, any Email that looks strange must be considered suspect

Do not Communicate Security Information electronically unless it is encrypted

Avoid Security Discussions on the Phone, take steps to **ensure no one can hear your conversation**

Ask your Suppliers (consultant, marketing agency, lawyer, accountant) how they Protect your Data!

Protect your Reputation and Copyrights

Some Intellectual Property Usurpation and Copyright Infringement can be the **start of Identity Theft or Phishing Attempts** (disguising oneself as a trustworthy entity in an electronic communication in order to gain access to Secure or Sensitive Information)

Every Social Network takes Intellectual Property theft very seriously (Report Misuse and they will Act!)

Most Web Hosting Companies will not tolerate Intellectual Property theft and Copyright Infringement (Report Misuse and they will Act!)

https://en.wikipedia.org/wiki/Online_Copyright_Infringement_Liability_Limitation_Act#Notice_from_copyright_owner

Part 4 | What you Can Do - Reputation

Protect your Reputation and Report Incidents

Monitor your Reputation Online, especially if someone is Faking your Identity, set Alerts (Monitoring Keyword, Name and Company Name) to Notify you Automatically (Daily, Weekly)

https://www.google.ca/alerts

Report Suspect Activity to the Royal Canadian Mounted Police (RCMP)

- Spam
- Phishing
- Scams
- Fraud

https://www.getcybersafe.gc.ca/cnt/rsrcs/rcvr-scm-en.aspx

Part 4 | What you Can Do - Reputation

Protect your Reputation and Copyrights

Monitor for Plagiarism of Content on your Website

https://www.copyscape.com/

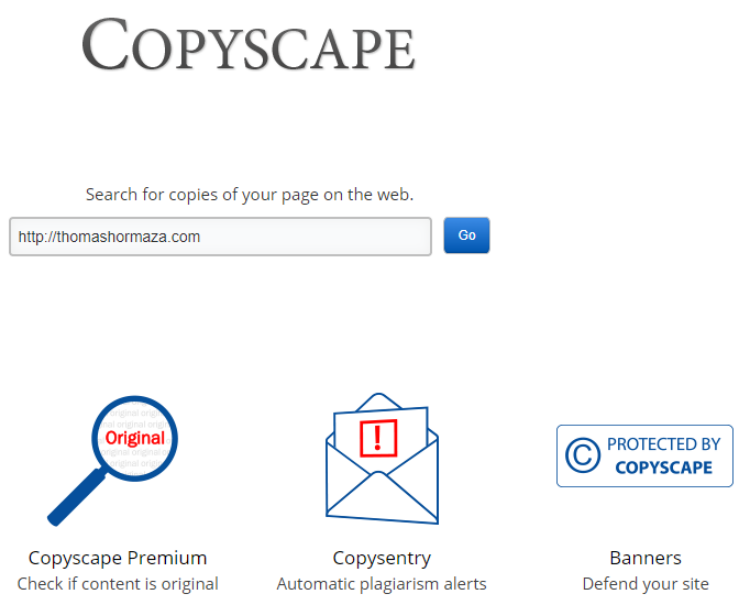
Protect your Intellectual Property

Register or Check Copyrights Database

Register or Check Trademarks Database

https://www.ic.gc.ca/app/opic-cipo/trdmrks/srch/home

https://www.ic.gc.ca/app/opic-cipo/cpyrghts/dsplySrch.do



Technology, Networks, WiFi and Servers

Hypertext Transfer Protocol Secure (HTTPS), encrypts communication on web server (i.e. credit cards)

Secure File Transfer Protocol (SFTP), SSH is a Secure Shell that encrypts when accessing server (eg. Ensures No one Can Sneak in While you Update a File on your Website)

Update your Software and Operating Systems, the most recent versions usually are more secure

Technology, Networks, WiFi and Servers

Secure wireless networks and Routers, change the Passwords regularly and use WPA2 or WPA3 (Wi-Fi Protected Access) versions

Firewalls monitor and control incoming and outgoing traffic (blocking if it detects threat), install it on servers as well as office devices

Multi Factor Authentication system that doublechecks eg. Password + Code received on your Cell

Run Virus Scans on the Network as well as on Devices

https://duo.com/product/multi-factor-authentication-mfa
https://www.getcybersafe.gc.ca/cnt/blg/pst-20171006-en.aspx

Tools, Scans and Monitoring

Denial of Service (DoS) Attack can halt your site unless you can block the Attack, most Hosting provides tools to block IP and locations in order to stop or reduce the effect of the attack

Automated Backup most Web Hosting Companies offer a Backup Service

Monitor Cloud Load with Tools such as Symantec Cloud Workload Protection

Other Vulnerabilities cross-site scripting XSS client side, URL, SQL with free (Pentest) or Paid Tools

https://www.symantec.com/products/hybrid-cloud-security
https://pentest-tools.com
https://www.ionos.ca/help/hosting/htaccess/deny-http-access-to-individual-ip-addresses/

Best Defense is to be Trained and Ready

Train All Staff concerning Security Best Practices

Company Procedures so Employees and Suppliers know that Security is also their Responsibility

Prepare a Plan so you know what to do if there is a Security Breach

Thanks
Stay in touch!

Join Agile Marketing Communities

https://www.linkedin.com/company/frenchmarketingcanada
https://www.linkedin.com/in/scrum-master
Thomas@FrenchMarketing.ca