FIPs and Fibs

SPISE Camp

Miti Mazmudar

Learning Outcomes

- List provincial and federal laws relevant to privacy.

Learning Outcomes

- List provincial and federal laws relevant to privacy.
- Outline which regulatory authorities you can reach out to about violations of these laws.

Learning Outcomes

- List provincial and federal laws relevant to privacy.
- Outline which regulatory authorities you can reach out to about violations of these laws.
- Describe Fair Information Principles (FIP).

Learning Outcomes

- List provincial and federal laws relevant to privacy.
- Outline which regulatory authorities you can reach out to about violations of these laws.
- Describe Fair Information Principles (FIP).
- Discuss and role-play examples violating FIPs.

Learning Outcomes

- List provincial and federal laws relevant to privacy.
- Outline which regulatory authorities you can reach out to about violations of these laws.
- Describe Fair Information Principles (FIP).
- Discuss and role-play examples violating FIPs.
- Given an example of a summarized case proceeding, determine which FIPs are violated in that proceeding.

Learning Outcomes

- List provincial and federal laws relevant to privacy.
- Outline which regulatory authorities you can reach out to about violations of these laws.
- Describe Fair Information Principles (FIP).
- Discuss and role-play examples violating FIPs.
- Given an example of a summarized case proceeding, determine which FIPs are violated in that proceeding.
- Complete a privacy risk assessment questionnaire.

Regulations

- PIPEDA:

Regulations

- PIPEDA:
- POPA:

Regulations

- PIPEDA:
- POPA:
- GDPR:

Regulations

- PIPEDA:

- POPA:
- GDPR:
- COPPA:

Regulations

- PIPEDA: Personal Information Protection and Electronic Documents Act. Canada's federal privacy law.
- POPA:
- GDPR:
- COPPA:

Regulations

- PIPEDA: Personal Information Protection and Electronic Documents Act. Canada's federal privacy law.
- POPA: Protection of Privacy Act. Alberta's privacy law.
- GDPR:
- COPPA:

Regulations

- PIPEDA: Personal Information Protection and Electronic Documents Act. Canada's federal privacy law.
- POPA: Protection of Privacy Act. Alberta's privacy law.
- GDPR: General Data Protection Regulation. Europe's privacy law.
- COPPA:

Regulations

- PIPEDA: Personal Information Protection and Electronic Documents Act. Canada's federal privacy law.
- POPA: Protection of Privacy Act. Alberta's privacy law.
- GDPR: General Data Protection Regulation. Europe's privacy law.
- COPPA: Children's Online Privacy Protection Act. US's federal privacy law for chilren.

Regulators

- OPC:

Regulators

- OPC:
- OIPCA:

Regulators

- OPC:
- OIPCA:
- DPA:

Regulators

- OPC:

- OIPCA:
- DPA:
- FTC:

Regulators

- OPC: Office of the Privacy Commissioner. Canada's federal privacy regulator. Enforces PIPEDA.
- OIPCA:
- DPA:
- FTC:

Regulators

- OPC: Office of the Privacy Commissioner. Canada's federal privacy regulator. Enforces PIPEDA.
- OIPCA: Office of the Information Privacy Commissioner of Alberta.
- DPA:
- FTC:

Regulators

- OPC: Office of the Privacy Commissioner. Canada's federal privacy regulator. Enforces PIPEDA.
- OIPCA: Office of the Information Privacy Commissioner of Alberta.
- DPA: Data Protection Authority. Each EU nation that enforces GDPR has one.
- FTC:

Regulators

- OPC: Office of the Privacy Commissioner. Canada's federal privacy regulator. Enforces PIPEDA.
- OIPCA: Office of the Information Privacy Commissioner of Alberta.
- DPA: Data Protection Authority. Each EU nation that enforces GDPR has one.
- FTC: Federal Trade Commission. American federal privacy regulator. Enforces COPPA.

Principle 1: Accountability

- Need to have support from higher-ups

Principle 1: Accountability

- Need to have support from higher-ups
- Have a privacy officer position / team

Principle 1: Accountability

- Need to have support from higher-ups
- Have a privacy officer position / team
- Whose job is to implement the remaining FIPs

Principle 1: Accountability

- Need to have support from higher-ups
- Have a privacy officer position / team
- Whose job is to implement the remaining FIPs
- Products designed by the organization should be reviewed by this person / team

Questionnaire

OPC: Start by using the following questionnaire:

- What personal information do we collect and is it sensitive? (Sensitive information may require extra protection.)

Questionnaire

OPC: Start by using the following questionnaire:

- What personal information do we collect and is it sensitive? (Sensitive information may require extra protection.)
- Why do we collect it?

Questionnaire

OPC: Start by using the following questionnaire:

- What personal information do we collect and is it sensitive? (Sensitive information may require extra protection.)
- Why do we collect it?
- How do we collect it?

Questionnaire

OPC: Start by using the following questionnaire:

- What personal information do we collect and is it sensitive? (Sensitive information may require extra protection.)
- Why do we collect it?
- How do we collect it?
- What do we use it for?

Questionnaire

OPC: Start by using the following questionnaire:

- What personal information do we collect and is it sensitive? (Sensitive information may require extra protection.)
- Why do we collect it?
- How do we collect it?
- What do we use it for?
- Where do we keep it?

Questionnaire

OPC: Start by using the following questionnaire:

- What personal information do we collect and is it sensitive? (Sensitive information may require extra protection.)
- Why do we collect it?
- How do we collect it?
- What do we use it for?
- Where do we keep it?
- How is it secured?

Questionnaire

OPC: Start by using the following questionnaire:

- What personal information do we collect and is it sensitive? (Sensitive information may require extra protection.)
- Why do we collect it?
- How do we collect it?
- What do we use it for?
- Where do we keep it?
- How is it secured?
- Who has access to or uses it?

Questionnaire

OPC: Start by using the following questionnaire:

- What personal information do we collect and is it sensitive? (Sensitive information may require extra protection.)
- Why do we collect it?
- How do we collect it?
- What do we use it for?
- Where do we keep it?
- How is it secured?
- Who has access to or uses it?
- Who do we share it with?

Questionnaire

OPC: Start by using the following questionnaire:

- What personal information do we collect and is it sensitive? (Sensitive information may require extra protection.)
- Why do we collect it?
- How do we collect it?
- What do we use it for?
- Where do we keep it?
- How is it secured?
- Who has access to or uses it?
- Who do we share it with?
- When is it deleted?

Example: Google

- An engineer at Google designed a feature that had a privacy problem (see later[1])

[1] https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2011/pipeda-2011-001/

Example: Google

- An engineer at Google designed a feature that had a privacy problem (see later[1])
- ✔ All external-facing products had to go through a "Product Counsel Review" program

[1] https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2011/pipeda-2011-001/

Example: Google

- An engineer at Google designed a feature that had a privacy problem (see later[1])
- ✔ All external-facing products had to go through a "Product Counsel Review" program
- ✖ The engineer did not go through this review: this product only had "superficial privacy problems"

[1] https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2011/pipeda-2011-001/

Example: Google

- An engineer at Google designed a feature that had a privacy problem (see later[1])

✔ All external-facing products had to go through a "Product Counsel Review" program

✖ The engineer did not go through this review: this product only had "superficial privacy problems"

✔ OPC: Google, make your tech leads of your teams do a privacy design document for each feature.

[1] https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2011/pipeda-2011-001/

Accountability: Lessons learnt

- Need to have support from higher-ups

Accountability: Lessons learnt

- Need to have support from higher-ups
- Have a privacy officer position / team

Accountability: Lessons learnt

- Need to have support from higher-ups
- Have a privacy officer position / team
- Whose job is to implement the remaining FIPs

Accountability: Lessons learnt

- Need to have support from higher-ups
- Have a privacy officer position / team
- Whose job is to implement the remaining FIPs
- *Products designed by the organization should be reviewed by this person / team*

Principle 2: Identifying Purposes

- The purposes for which the personal information is being collected

Principle 2: Identifying Purposes

- The purposes for which the personal information is being collected must be identified by the organization

Principle 2: Identifying Purposes

- The purposes for which the personal information is being collected must be identified by the organization **before** or (latest) at the time of collection.

Principle 2: Identifying Purposes

- The purposes for which the personal information is being collected must be identified by the organization **before** or (latest) at the time of collection.

✖ Collect lots of data now, figure out what you'll use it for later.

Principle 2: Identifying Purposes

- The purposes for which the personal information is being collected must be identified by the organization **before** or (latest) at the time of collection.

✖ Collect lots of data now, figure out what you'll use it for later.

✔ Narrowly defined purposes are better. Some examples:

Principle 2: Identifying Purposes

- The purposes for which the personal information is being collected must be identified by the organization **before** or (latest) at the time of collection.

✖ Collect lots of data now, figure out what you'll use it for later.

✔ Narrowly defined purposes are better. Some examples:
  - opening an account;

Principle 2: Identifying Purposes

- The purposes for which the personal information is being collected must be identified by the organization **before** or (latest) at the time of collection.

✖ Collect lots of data now, figure out what you'll use it for later.

✔ Narrowly defined purposes are better. Some examples:

  - opening an account;
  - verifying a person's creditworthiness;

Principle 2: Identifying Purposes

- The purposes for which the personal information is being collected must be identified by the organization **before** or (latest) at the time of collection.

✖ Collect lots of data now, figure out what you'll use it for later.

✔ Narrowly defined purposes are better. Some examples:

  - opening an account;
  - verifying a person's creditworthiness;
  - providing benefits to employees;

Principle 2: Identifying Purposes

- The purposes for which the personal information is being collected must be identified by the organization **before** or (latest) at the time of collection.

✖ Collect lots of data now, figure out what you'll use it for later.

✔ Narrowly defined purposes are better. Some examples:

  - opening an account;
  - verifying a person's creditworthiness;
  - providing benefits to employees;
  - figuring if a customer is eligible for special offers or discounts.

Principle 3: Consent

- People need to know what data items are **collected**,

Principle 3: Consent

- People need to know what data items are **collected**, **used**, or
- They need to know the **purposes** for which their data is collected, used or shared.

Principle 3: Consent

- People need to know what data items are **collected**, **used**, or **shared,**

- They need to know the **purposes** for which their data is collected, used or shared.
- They need to be able to consent **meaningfully**.

Principle 3: Consent

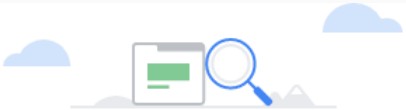
- People need to know what data items are **collected**, **used**, or **shared,** as well as which other parties their data items are being shared with.
- They need to know the **purposes** for which their data is collected, used or shared.
- They need to be able to consent **meaningfully**.
- **Opt-out** by default, not opt-in

Example: Google Settings

A guide of your privacy choices

Take a guided tour of key privacy and security controls. For more options, go to individual settings.

Example: Google Settings



Choose your search and browsing quality

Make searches and browsing better

When on

- You'll browse faster because content is proactively loaded based on your current web page visit
- You'll get improved suggestions in the address bar

Things to consider

- URLs that you visit are sent to Google to predict what sites you might visit next
- If you also share Chrome usage reports, those reports include the URLs that you visit

Example: Google Settings

Choose your Safe Browsing protection

Enhanced protection
Faster, proactive protection against dangerous websites, downloads and extensions. Warns you about password breaches. Requires browsing data to be sent to Google.

Standard protection
Standard protection against websites, downloads and extensions that are known to be dangerous

When on

Detects and warns you about dangerous events when they happen

Things to consider

If a site tries to steal your password, or when you download a harmful file, Chrome

Example: Google Settings

Choose your Safe Browsing protection

Enhanced protection

Faster, proactive protection against dangerous websites, downloads and extensions. Warns you about password breaches. Requires browsing data to be sent to Google.

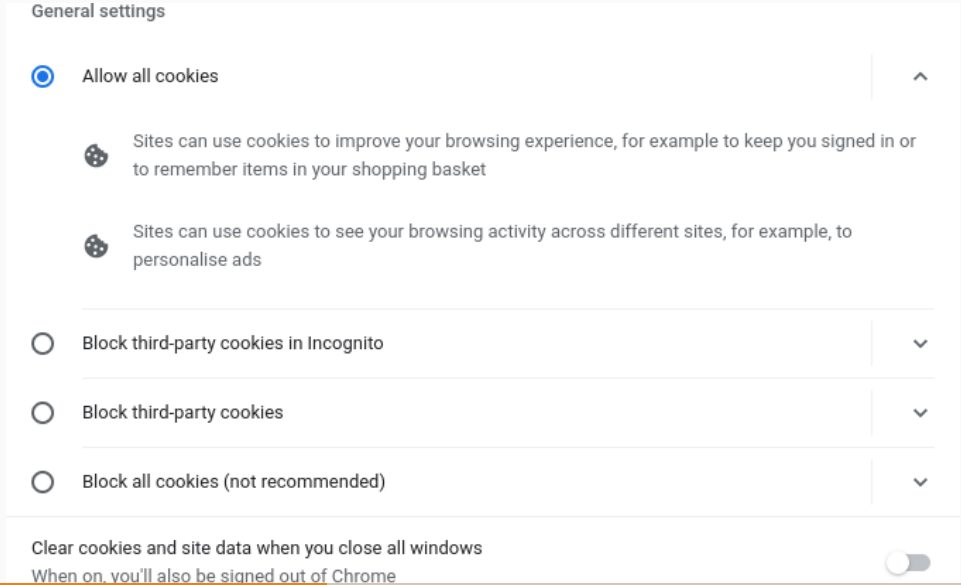
When on

- Predicts and warns you about dangerous events before they happen
- Keeps you safe on Chrome and may be used to improve your security in other Google apps when you are signed in

Things to consider

- Sends URLs to Safe Browsing to check them
- Also sends a small sample of pages, downloads, extension activity and system information to help discover new threats

Example: Google Settings



Principle 3: Consent meaningfully

Meaningful consent is:

- **freely given**: must be able to refuse or withdraw consent without detriment.

Principle 3: Consent meaningfully

Meaningful consent is:

- **freely given**: must be able to refuse or withdraw consent without detriment.
- **specific**: can consent to different purposes and data items separately

Principle 3: Consent meaningfully

Meaningful consent is:

- **freely given**: must be able to refuse or withdraw consent without detriment.
- **specific**: can consent to different purposes and data items separately
- **informed**: person should know and understand what data items will be collected, why, and how they'll be processed

Principle 3: Consent meaningfully

Meaningful consent is:

- **freely given**: must be able to refuse or withdraw consent without detriment.
- **specific**: can consent to different purposes and data items separately
- **informed**: person should know and understand what data items will be collected, why, and how they'll be processed
- **unambiguous**, not as follows:

Principle 3: Consent meaningfully

Meaningful consent is:

- **freely given**: must be able to refuse or withdraw consent without detriment.
- **specific**: can consent to different purposes and data items separately
- **informed**: person should know and understand what data items will be collected, why, and how they'll be processed
- **unambiguous**, not as follows:
  - ✖ implicitly (continuing to browse means you agree)

Principle 3: Consent meaningfully

Meaningful consent is:

- **freely given**: must be able to refuse or withdraw consent without detriment.
- **specific**: can consent to different purposes and data items separately
- **informed**: person should know and understand what data items will be collected, why, and how they'll be processed
- **unambiguous**, not as follows:
  - ✖ implicitly (continuing to browse means you agree)
  - ✖ pre-checked boxes

Principle 3: Consent meaningfully

Meaningful consent is:

- **freely given**: must be able to refuse or withdraw consent without detriment.
- **specific**: can consent to different purposes and data items separately
- **informed**: person should know and understand what data items will be collected, why, and how they'll be processed
- **unambiguous**, not as follows:
  - ✖ implicitly (continuing to browse means you agree)
  - ✖ pre-checked boxes
  - ✖ or doing nothing

Principle 3: Consent meaningfully

Meaningful consent is:

- **freely given**: must be able to refuse or withdraw consent without detriment.
- **specific**: can consent to different purposes and data items separately
- **informed**: person should know and understand what data items will be collected, why, and how they'll be processed
- **unambiguous**, not as follows:
  - ✖ implicitly (continuing to browse means you agree)
  - ✖ pre-checked boxes
  - ✖ or doing nothing
- when *revoking* consent is as easy as granting it (bad e.g., opting in with a click, cancelling with an email, phone call)

Dark or deceptive design patterns

- Tricks used in websites and apps that make you do things that you didn't mean or want.

Dark or deceptive design patterns

- Tricks used in websites and apps that make you do things that you didn't mean or want.
- Used to get people's consent misleadingly.

Dark or deceptive design patterns

- Tricks used in websites and apps that make you do things that you didn't mean or want.
- Used to get people's consent misleadingly.
- Following examples from https://www.deceptive.design

Dark or deceptive design patterns

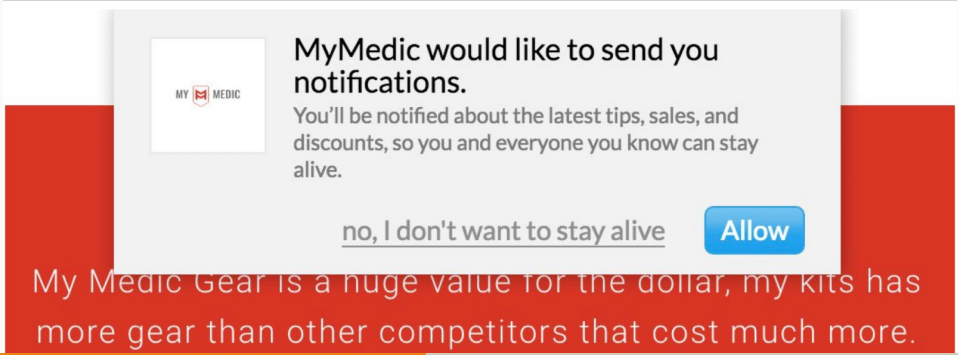
- Tricks used in websites and apps that make you do things that you didn't mean or want.
- Used to get people's consent misleadingly.
- Following examples from https://www.deceptive.design
- Other resources: https://darkpatternstipline.org/

Consent Dark Patterns

- Only the opt-in option is present on the initial cookie dialog
- The background colour of the opt-in button leads to it being highlighted more compared to the opt-out button
- Dialog obstructs most of the window
- Dialog text is difficult to read
- Dialog hides some options behind a “more options” button
- Ambiguous close ($\times$) button is present on the dialog (does that mean opt-in or opt-out?)
- Multiple distinct cookie dialogs present on a page
- At least one preference slider is enabled by default

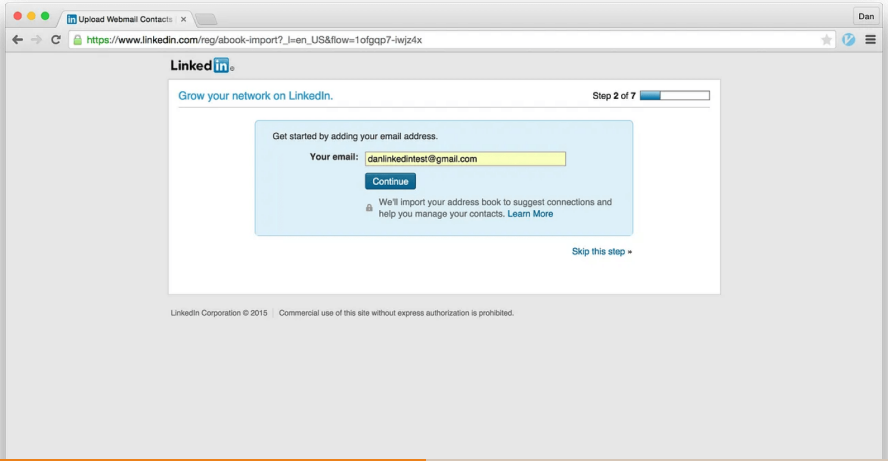
Dark design pattern: confirmshaming

Use uncomfortable emotions to influence decision making



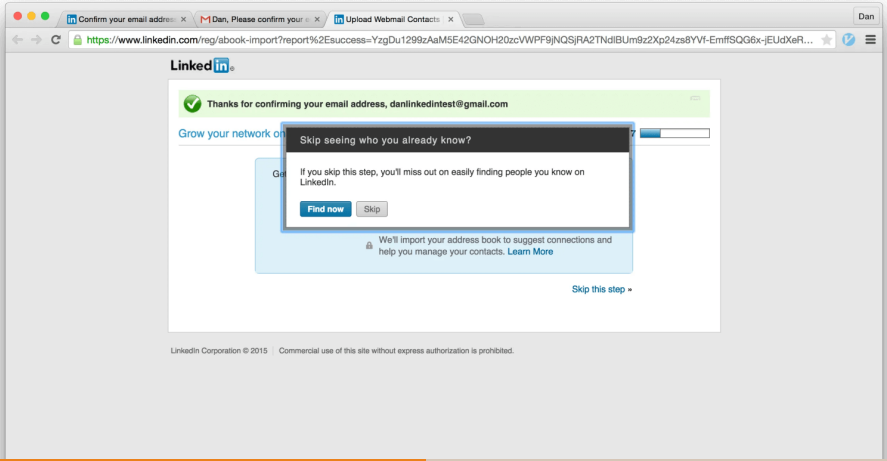
Dark design pattern: forced action

Offer users something they want but make them agree to something in return.



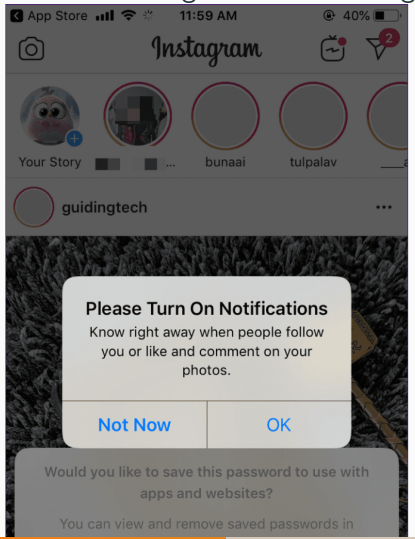
Dark design pattern: forced action

Offer users something they want but make them agree to something in return.



Dark design pattern: nagging

Repeatedly remind users who haven't agreed to something until they finally relent.



Principle 4: Limiting collection

- Limit collecting personal information

Principle 4: Limiting collection

- Limit collecting personal information to that which is needed for the purposes identified by the organization

Principle 4: Limiting collection

- Limit collecting personal information to that which is needed for the purposes identified by the organization
- Why? Less data $\implies$ less data breaches

Principle 4: Limiting collection

- Limit collecting personal information to that which is needed for the purposes identified by the organization
- Why? Less data $\implies$ less data breaches
- Principle 2: We identified what data items we would be collecting & what purposes we would be collecting them for.

Principle 4: Limiting collection

- Limit collecting personal information to that which is needed for the purposes identified by the organization
- Why? Less data $\implies$ less data breaches
- Principle 2: We identified what data items we would be collecting & what purposes we would be collecting them for.
- Principle 4: Do you need this data item for a primary purpose? If not:

Principle 4: Limiting collection

- Limit collecting personal information to that which is needed for the purposes identified by the organization
- Why? Less data $\implies$ less data breaches
- Principle 2: We identified what data items we would be collecting & what purposes we would be collecting them for.
- Principle 4: Do you need this data item for a primary purpose? If not:
  - Don't collect it!

Principle 4: Limiting collection

- Limit collecting personal information to that which is needed for the purposes identified by the organization
- Why? Less data $\implies$ less data breaches
- Principle 2: We identified what data items we would be collecting & what purposes we would be collecting them for.
- Principle 4: Do you need this data item for a primary purpose? If not:
  - Don't collect it!
  - If you've collected it, then you should delete it!

Principle 4: Limiting collection

- Limit collecting personal information to that which is needed for the purposes identified by the organization
- Why? Less data $\implies$ less data breaches
- Principle 2: We identified what data items we would be collecting & what purposes we would be collecting them for.
- Principle 4: Do you need this data item for a primary purpose? If not:
  - Don't collect it!
  - If you've collected it, then you should delete it!
- Also known as **data minimization**

Example: Driver's license & shopping

- Person: Goes to register at a store or buy something from a store.

[2] https://www.priv.gc.ca/en/privacy-topics/sins-and-drivers-licences/drivers-licences/guide_edl/

Example: Driver's license & shopping

- Person: Goes to register at a store or buy something from a store.
- Store: Show us your drivers license. We will write down your drivers license number.

[2] https://www.priv.gc.ca/en/privacy-topics/sins-and-drivers-licences/drivers-licences/guide_edl/

Example: Driver's license & shopping

- Person: Goes to register at a store or buy something from a store.
- Store: Show us your drivers license. We will write down your drivers license number.
- Store: The purpose is to verify your identity & to protect our business from credit card fraud.

[2] https://www.priv.gc.ca/en/privacy-topics/sins-and-drivers-licences/drivers-licences/guide_edl/

Example: Driver's license & shopping

- Person: Goes to register at a store or buy something from a store.
- Store: Show us your drivers license. We will write down your drivers license number.
- Store: The purpose is to verify your identity & to protect our business from credit card fraud.
- Person: Okay I will show you my drivers license, but do you really need to write it down?

[2] https://www.priv.gc.ca/en/privacy-topics/sins-and-drivers-licences/drivers-licences/guide_edl/

Example: Driver's license & shopping

- Person: Goes to register at a store or buy something from a store.
- Store: Show us your drivers license. We will write down your drivers license number.
- Store: The purpose is to verify your identity & to protect our business from credit card fraud.
- Person: Okay I will show you my drivers license, but do you really need to write it down?
- OPC[2]: No, they don't — the employee can check that the name on the credit card and the driver's license match.

[2] https://www.priv.gc.ca/en/privacy-topics/sins-and-drivers-licences/drivers-licences/guide_edl/

Example: Driver's license & shopping

- Person: Goes to register at a store or buy something from a store.
- Store: Show us your drivers license. We will write down your drivers license number.
- Store: The purpose is to verify your identity & to protect our business from credit card fraud.
- Person: Okay I will show you my drivers license, but do you really need to write it down?
- OPC[2]: No, they don't — the employee can check that the name on the credit card and the driver's license match.
- OPC: The employee can then place their initials on customer forms, confirming that they have checked the customer's driver's license.

[2] https://www.priv.gc.ca/en/privacy-topics/sins-and-drivers-licences/drivers-licences/guide_edl/

Example: Driver's license & shopping

- Person: Goes to register at a store or buy something from a store.
- Store: Show us your drivers license. We will write down your drivers license number.
- Store: The purpose is to verify your identity & to protect our business from credit card fraud.
- Person: Okay I will show you my drivers license, but do you really need to write it down?
- OPC[2]: No, they don't — the employee can check that the name on the credit card and the driver's license match.
- OPC: The employee can then place their initials on customer forms, confirming that they have checked the customer's driver's license.
- OPC: "Recording the licence number does not provide any further authentication of the individual's identity."

[2] https://www.priv.gc.ca/en/privacy-topics/sins-and-drivers-licences/drivers-licences/guide_edl/

Example: Driver's license & shopping

- OPC: About fraud deterrence — most people will not commit an offense and so their information will not ever be required.

Example: Driver's license & shopping

- OPC: About fraud deterrence — most people will not commit an offense and so their information will not ever be required.
- OPC: You first need to show that recording down the license number deters fraud.

Example: Driver's license & shopping

- OPC: About fraud deterrence — most people will not commit an offense and so their information will not ever be required.
- OPC: You first need to show that recording down the license number deters fraud.
- Store: Okay there are some bad buyers that keep returning items without a receipt. So we ask everyone to provide their driver's license number.

Example: Driver's license & shopping

- OPC: About fraud deterrence — most people will not commit an offense and so their information will not ever be required.
- OPC: You first need to show that recording down the license number deters fraud.
- Store: Okay there are some bad buyers that keep returning items without a receipt. So we ask everyone to provide their driver's license number.
- OPC: Okay but the driver's licence number was not supposed to be a numeric identifier for statistical analysis of shopping return habits.

Example: Driver's license & shopping

- OPC: About fraud deterrence — most people will not commit an offense and so their information will not ever be required.
- OPC: You first need to show that recording down the license number deters fraud.
- Store: Okay there are some bad buyers that keep returning items without a receipt. So we ask everyone to provide their driver's license number.
- OPC: Okay but the driver's licence number was not supposed to be a numeric identifier for statistical analysis of shopping return habits.
- OPC: Any other unique identifier that you can generate and record for each consumer, is sufficient.

Principle 5: Limiting use, sharing & retention

- Personal information can *only* be used or shared for the purposes for which it was collected.

Principle 5: Limiting use, sharing & retention

- Personal information can *only* be used or shared for the purposes for which it was collected.

✖ Collect data for (primary) purpose X, use it or share it with others for (secondary) purpose Y.

Principle 5: Limiting use, sharing & retention

- Personal information can *only* be used or shared for the purposes for which it was collected.
- ✖ Collect data for (primary) purpose X, use it or share it with others for (secondary) purpose Y.
- Personal information *must only* be kept as long as required to serve those purposes.

Principle 5: Limiting use, sharing & retention

- Personal information can *only* be used or shared for the purposes for which it was collected.

✖ Collect data for (primary) purpose X, use it or share it with others for (secondary) purpose Y.

- Personal information *must only* be kept as long as required to serve those purposes.

✖ Collect data for (primary) purpose X, keep it in case we want to use it later.

Principle 5: Limiting use, sharing & retention

- Personal information can *only* be used or shared for the purposes for which it was collected.
- ✖ Collect data for (primary) purpose X, use it or share it with others for (secondary) purpose Y.
- Personal information *must only* be kept as long as required to serve those purposes.
- ✖ Collect data for (primary) purpose X, keep it in case we want to use it later.
- Why? Less data $\implies$ less data breaches

Principle 5: Takeaways

Collected data item for purpose X?

Principle 5: Takeaways

Collected data item for purpose X?

- Limiting use: Only use it for purpose X.

Principle 5: Takeaways

Collected data item for purpose X?

- Limiting use: Only use it for purpose X.
- Limiting sharing: Got users' consent to share it with party Y? Only share it with party Y for purpose X.

Principle 5: Takeaways

Collected data item for purpose X?

- Limiting use: Only use it for purpose X.
- Limiting sharing: Got users' consent to share it with party Y? Only share it with party Y for purpose X.
- Limiting retention: Retain it only until purpose X is fulfilled. Delete it afterwards!

Principle 7: Safeguards

- Question: What security controls do you know?

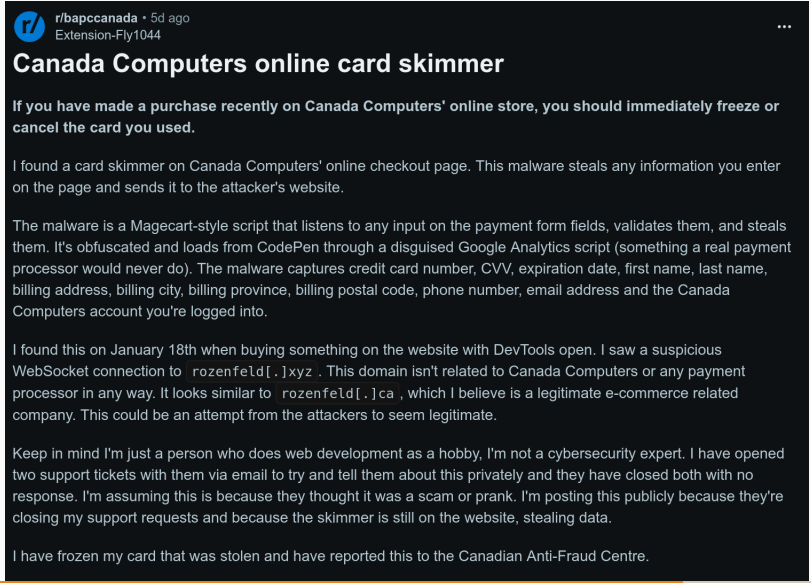
Principle 7: Safeguards

- Question: What security controls do you know?
- Encryption. Access control. Firewalls. Passwords.

Principle 7: Safeguards

- Question: What security controls do you know?
- Encryption. Access control. Firewalls. Passwords.
- Not enough to just set them up — maintain them, do security audits.

Example: Canada Computers breach



r/bapccanada • 5d ago
Extension-Fly1044

Canada Computers online card skimmer

If you have made a purchase recently on Canada Computers' online store, you should immediately freeze or cancel the card you used.

I found a card skimmer on Canada Computers' online checkout page. This malware steals any information you enter on the page and sends it to the attacker's website.

The malware is a Magecart-style script that listens to any input on the payment form fields, validates them, and steals them. It's obfuscated and loads from CodePen through a disguised Google Analytics script (something a real payment processor would never do). The malware captures credit card number, CVV, expiration date, first name, last name, billing address, billing city, billing province, billing postal code, phone number, email address and the Canada Computers account you're logged into.

I found this on January 18th when buying something on the website with DevTools open. I saw a suspicious WebSocket connection to `rozenfeld[.]xyz`. This domain isn't related to Canada Computers or any payment processor in any way. It looks similar to `rozenfeld[.]ca`, which I believe is a legitimate e-commerce related company. This could be an attempt from the attackers to seem legitimate.

Keep in mind I'm just a person who does web development as a hobby, I'm not a cybersecurity expert. I have opened two support tickets with them via email to try and tell them about this privately and they have closed both with no response. I'm assuming this is because they thought it was a scam or prank. I'm posting this publicly because they're closing my support requests and because the skimmer is still on the website, stealing data.

I have frozen my card that was stolen and have reported this to the Canadian Anti-Fraud Centre.

Example: Canada Computers breach

UPDATE (Jan 22, 4:54 PM EST):

The skimmer seems to have been removed from the live site. As of 4:54 PM EST, the checkout page no longer contains the malicious script or connections to `rozenfeld[.]xyz`. However, there is archived proof of this on Archive.org from December 31st 2025 that confirms the skimmer was on the checkout page.

Archive link: https://web.archive.org/web/20251231195438/https://www.canadacomputers.com/en/

Archive timestamp: Wed, 31 Dec 2025 19:54:38 GMT

This means the skimmer was active for at least 3 weeks.

Canada Computers has yet to acknowledge this breach or notify customers at all.

The latest snapshot I found on Archive.org that didn't have the skimmer was made on December 8 2025. If you bought anything on their online store between Dec 8 and Jan 22, your card info has been stolen and you should take the precautions I recommended at the top of the post (cancel/freeze). Even if you bought something before December 8 on the online store, I'd watch my bank statements very closely since their website has a history of data breaches and bad practices.

4

[4] https://www.reddit.com/r/bapccanada/comments/1qk4axy/canada_computers_online_card_skimmer/

Takeaways: Responsible Disclosure

What does this breach report get right?

- Described the attack vector.

Takeaways: Responsible Disclosure

What does this breach report get right?

- Described the attack vector.
- Mentioned when the attack was discovered.

Takeaways: Responsible Disclosure

What does this breach report get right?

- Described the attack vector.
- Mentioned when the attack was discovered.
- Estimated when the attack might have occurred.

Takeaways: Responsible Disclosure

What does this breach report get right?

- Described the attack vector.
- Mentioned when the attack was discovered.
- Estimated when the attack might have occurred.
- Informed the business about the attack.

Example: Canada Computers response

Received Jan 26th:

We are writing to tell you about a data security incident that may have exposed certain of your personal information to an unauthorized intruder.

What Happened and What Information was Involved

On Friday, January 23, 2026, we discovered that there had been unauthorized access to portion of our system, which may have compromised the security of a few of our online customers' information. We believe that an unauthorized user may have gained access to certain customer information, including email addresses, first and last names and possibly credit card numbers. We do not have any evidence that this information has been used fraudulently.

What We Are Doing to Protect You

Our systems have been thoroughly vetted and further enhancement to our security systems have been implemented. Our systems were put through vigorous testing by our IT team to ensure there are no current vulnerabilities.

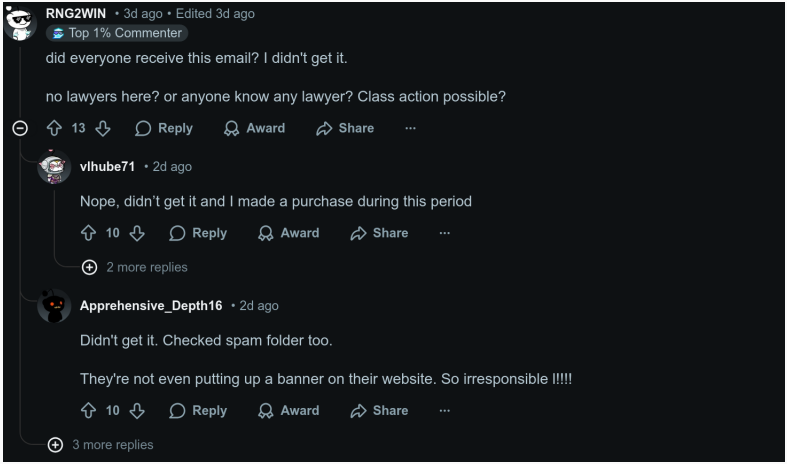
What You Can Do

We strongly encourage you to be vigilant in protecting your personal information by changing all of your website and computer passwords and check your bank and credit card statements to see if there have been any unusual or unauthorized transactions or activity. You may also wish to contact your bank or credit card company to cancel your card and request a new one.

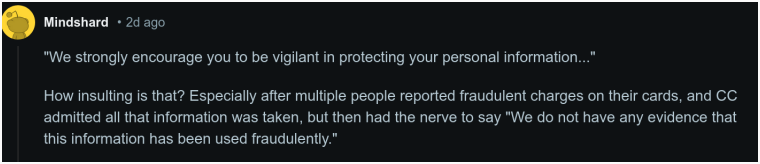
Please rest assured that our customers' well-being and the security of their personal information are our highest priorities. We apologize for any inconvenience this incident may cause you and thank you for your understanding and patience.

For More Information

Example: Reactions to Canada Computers response



Example: Reactions to Canada Computers response

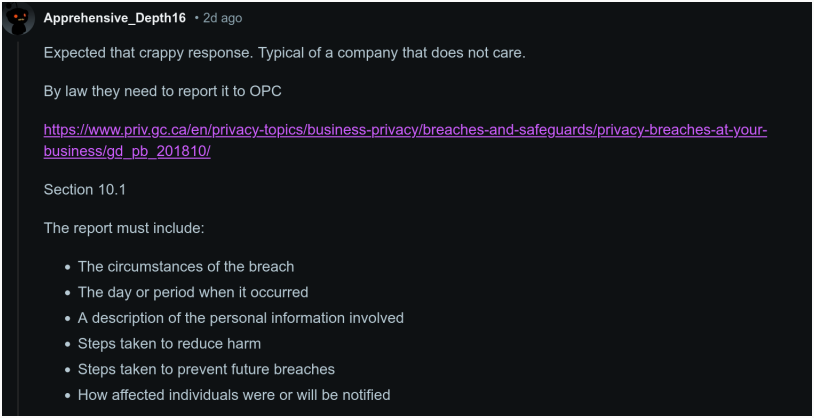


Mindshard • 2d ago

"We strongly encourage you to be vigilant in protecting your personal information..."

How insulting is that? Especially after multiple people reported fraudulent charges on their cards, and CC admitted all that information was taken, but then had the nerve to say "We do not have any evidence that this information has been used fraudulently."

Example: Reactions to Canada Computers response



Apprehensive_Depth16 • 2d ago

Expected that crappy response. Typical of a company that does not care.

By law they need to report it to OPC

https://www.priv.gc.ca/en/privacy-topics/business-privacy/breaches-and-safeguards/privacy-breaches-at-your-business/gd_pb_201810/

Section 10.1

The report must include:

- The circumstances of the breach
- The day or period when it occurred
- A description of the personal information involved
- Steps taken to reduce harm
- Steps taken to prevent future breaches
- How affected individuals were or will be notified

Takeaways: Security Incident Response

What did Canada Computers do wrong?

- ✖ Did not regularly audit their site beforehand.

Takeaways: Security Incident Response

What did Canada Computers do wrong?

- ✖ Did not regularly audit their site beforehand.
- ✖ Did not communicate back with the person who responsibly disclosed the attack.

Takeaways: Security Incident Response

What did Canada Computers do wrong?

- ✖ Did not regularly audit their site beforehand.
- ✖ Did not communicate back with the person who responsibly disclosed the attack.
- ✖ Did not take into account customers' complaints of their Credit Cards being used fraudulently.

Takeaways: Security Incident Response

What did Canada Computers do wrong?

- ✖ Did not regularly audit their site beforehand.
- ✖ Did not communicate back with the person who responsibly disclosed the attack.
- ✖ Did not take into account customers' complaints of their Credit Cards being used fraudulently.
- ✖ Not all potentially impacted customers received their email.

Takeaways: Security Incident Response

What did Canada Computers do wrong?

- ✖ Did not regularly audit their site beforehand.
- ✖ Did not communicate back with the person who responsibly disclosed the attack.
- ✖ Did not take into account customers' complaints of their Credit Cards being used fraudulently.
- ✖ Not all potentially impacted customers received their email.
- ✖ Put responsibility of securing account & financial information onto consumers.

Takeaways: Security Incident Response

What did Canada Computers do wrong?

- ✖ Did not regularly audit their site beforehand.
- ✖ Did not communicate back with the person who responsibly disclosed the attack.
- ✖ Did not take into account customers' complaints of their Credit Cards being used fraudulently.
- ✖ Not all potentially impacted customers received their email.
- ✖ Put responsibility of securing account & financial information onto consumers.
- ✖ May not have informed OPC of this breach — even though there's "real risk of significant harm".

Principle 8: Openness

- Your privacy policy should be .

Principle 8: Openness

- Your privacy policy should be available, .

Principle 8: Openness

- Your privacy policy should be available, easily accessible .

Principle 8: Openness

- Your privacy policy should be available, easily accessible and clear.

Principle 8: Openness

- Your privacy policy should be available, easily accessible and clear.
- Include your point-of-contact privacy officer (Principle 1 on Accountability).

Principle 8: Openness

- Your privacy policy should be available, easily accessible and clear.
- Include your point-of-contact privacy officer (Principle 1 on Accountability).
- Include how a user can access all the information that you have about them (Principle 9 on Individual Access).

Principle 8: Openness

- Your privacy policy should be available, easily accessible and clear.
- Include your point-of-contact privacy officer (Principle 1 on Accountability).
- Include how a user can access all the information that you have about them (Principle 9 on Individual Access).
- Include how a user can correct this information about them (Principle 6 on Accuracy).

Worksheet

1. Each team picks one of the following summarized case proceedings: Google Street View cars, Twitter, BetterHelp, Mariott and Apple.

Worksheet

1. Each team picks one of the following summarized case proceedings: Google Street View cars, Twitter, BetterHelp, Mariott and Apple.
2. Read through the background of the case, and at the end of the activity, you'll be asked to role-play each case and answer the questions for each case. You will figure out which FIPs are violated in that case.

Worksheet

1. Each team picks one of the following summarized case proceedings: Google Street View cars, Twitter, BetterHelp, Mariott and Apple.
2. Read through the background of the case, and at the end of the activity, you'll be asked to role-play each case and answer the questions for each case. You will figure out which FIPs are violated in that case.
3. **Every group** also solves the last question (Canada Computers). In this question, you'll complete a privacy risk assessment questionnaire.