Security Awareness Training

Jane's Handbook for Staff Members

Introduction

Did you know that 1 in 5 Canadian businesses reported that they were impacted by a cybersecurity incident?

With the increase of technology and cloud-based systems, this also comes with an increase in cyber-attacks, and so we've created our own security awareness training to educate everyone on how to keep their data secure.

As we go through the training, we'll learn more about the types of attacks, how we can prevent them, and what to do in an event when something does happen. Are you ready?

Let's get started!

Table of Contents

Password Hygiene

Getting started

As we go through this section, try and answer the following questions to familiarize yourself with password protection:

- **What does having good password hygiene mean?**
- **How do we keep our passwords safe?**
- **What do I do if my password is leaked?**

What is Password Hygiene?

Password hygiene is the practice of making account passwords secure. In this section, we'll be going over the best practices for securing passwords so that you can practice good password hygiene.

Keeping your passwords well protected will keep them away from attackers and keep them safe from unwanted eyes.

Why is it important to have good password hygiene?

Password hygiene is important because passwords protect your most sensitive data: credit cards, address, social information, health data—everything! Imagine if that data went to the wrong hands, then attackers would have more information, not only about you, but even the people you know too.

Jimmy Kimmel shows how easy it is for people to provide them with their password information through social engineering.

Watch Jimmy Kimmel's "What's Your Password?"

Story Time

An example of poor password hygiene was the Equifax breach in 2017. Equifax is a credit check service and **the breach exposed personally identifiable information of nearly 150 million users in the United States, Canada, and the UK.**

EQUIFAX

The cause? Equifax used the default username “admin” and set the password to--you guessed it, “admin.” Because there was also no multi-factor authentication, someone was able to access Equifax’s portal and retrieved roughly 209,000 credit card numbers, as well as social security and driver’s license numbers.

As a result, a class-action lawsuit was filed in the United States. The class-action lawsuit calls this, “a sure-fire way to get hacked,” and they’re not wrong. Millions of users now have their data exposed, something that could have easily been prevented if they had better security practices in place.

> *Millions of users have now their data exposed. Let’s make sure you’re not another case study.*

Story Recap

This is an example of a company that failed to implement adequate security practices. Anyone familiar with security knows that “admin” is typically the default password and incredibly easy for someone to guess.

This is why it’s incredibly important that we are using strong passwords and storing them in a place that’s secure and protected.

Keep It Confidential

One account, one password

Think about a time where you may have heard of a data breach, where account credentials are leaked. Imagine if a criminal had those credentials and was then able to access all of your other accounts.

By using unique passwords for each account, you add an extra layer of security and minimize further risk of exposure if your credentials are stolen.

Image credit: 1password.com

No sharing

Contrary to what you were told when you were younger--when it comes to passwords, sharing is not caring. So do not share your passwords with anyone, ever. This includes your friends, coworkers, IT staff or even your spouse/partner. Your password should only be known by you.

Keep It Secure

When it comes to securing passwords, the best advice we have is to refrain from writing it down on a piece of paper. These can easily be found and land in the wrong hands. Instead, we recommend using a password manager (i.e. LastPass or 1Password) to store passwords securely.

🏆 You've completed this section!

Great! You've now completed the Password Protection section. We hope you found the information helpful and can provide you with steps to further secure your passwords.

Device Protection

Getting Started

As we go through this section, we will be learning more about how we can protect the devices that we use every day. Try and answer the following questions to familiarize yourself with device protection:

- **How do we keep our devices safe?**
- **What do you do if you see an unknown device on the floor?**

What is Device Protection?

Our devices hold a lot of personal information: who our friends and family are, what we like or don't like, banking information—you name it! The devices that we use every day is how we stay connected with another. So it's essential to protect these devices because it not only protects you, but everyone else you know as well.

Did you know that Jane has a Privacy quick key?

Stop those wandering eyes in their tracks by clicking Shift + P on your keyboard to blur out private patient information on your schedule.

Protecting Devices

Keep your eyes on it

One of the key things that we can do to keep our devices well protected is never to leave the device unattended. It's also a good habit to be aware of your surroundings when viewing sensitive information in a public space to keep our screens away from wandering eyes.

Story Time

Device protection not only means that we keep it away from attackers, but it also includes making sure that attackers can't get to our devices too. Let's listen to Leanne's story.

Leanne is heading to work and just arrived outside the Jane office, and notices a USB drive on the floor. She's wondering if it belongs to one of her coworkers, so she picks it up and brings it in.

Curious to know who it belongs to, she plugs in the USB drive to her computer. **Was this a good idea?**

Story Recap

Sometimes, when someone finds a USB drive on the floor, they plug it into their computer in hopes of returning it to the rightful owner. And that's what Leanne did.

Though Leanne's intentions were good, the USB drive could have malicious code that could lead to a data breach. This type of attack is called a USB drop attack.

Here are two examples of attacks that could happen when we open a USB drive:

Malicious code

In the most basic USB drop attacks, the user clicks on one of the files. This unleashes a malicious code that automatically activates upon viewing and can download further malware from the Internet.

Social engineering

The file takes the thumb drive user to a phishing site, which tricks them into handing over their login credentials.

And these files can be well disguised too. Imagine if there was a file named “Joe_Resume.pdf.” Wouldn’t that seem like a safe and useful file to open to help you return the device to its rightful owner? Except, as you now know, that same file could be set up to deliver malicious code to your device.

🏆 You’ve completed this section!

Awesome! Another one completed. Now that we’ve gone through the Device Protection section, we hope that we provided you with some helpful tips to secure your devices.

Malware

Getting Started

As we go through this section, come back to these questions listed below to see how confident you are in answering them. By taking this extra step, we can keep our computers safe from malicious software.

- **What malware is.**
- **The five different types of common malware.**
- **How we prevent malware from installing on our devices.**

What is Malware?

Before we get started answering, “how do we keep our devices safe?”, we need to understand what malware is.

Malware is malicious software, designed to damage, disrupt, or gain unauthorized access to a device.

There are many different types of malware like viruses, adware, spyware, worms, etc., which you can learn more about here: https://www.upguard.com/blog/types-of-malware

Instead of going through all the different types of malware, we’ll be touching on five of the most common ones so that we know what to be on the lookout for.

Five Most Common Types of Malware:

1. Worm

2. Spyware

3. Keylogger

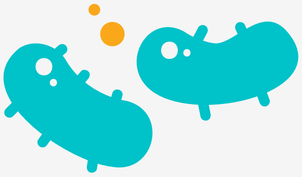
4. Ransomware

5. Trojan

Worm

What is a worm?

Worms are a type of malware similar to viruses where they self-replicate to spread to other computers over a network, usually causing harm by destroying data and files.



Stuxnet

Stuxnet was found in 2010. Though unlike any other virus or worm that targets computers, this one escaped the digital realm and entered into physical destruction.

Who was it targeting?

Although neither the U.S. and Isreal government openly admitted responsibility, the worm was intended as a tool to derail, or at least delay, the Iranian program to develop nuclear weapons.

How did it spread?

Stuxnet traveled on USB sticks and spread through Microsoft Windows computers.

What was the outcome?

Stuxnet reportedly ruined almost one-fifth of Iran’s nuclear centrifuges. Targeting industrial control systems, the worm infected over 200,000 computers and caused 1,000 machines to physically degrade.

> *Stuxnet infected 200k computers and caused 1k machines to physically degrade.*

Spyware

What is spyware?

Spyware is malware that secretly observes a user's activities without permission and reports it to the software's author. By doing so it can collect sensitive information like usernames, passwords, or credit card details.

DarkHotel

For the last few years, a group has been targeting executives and government officials staying at high-end hotels. They hack their computers and grab their files, add a keylogger, and install a virus that can then spread within the victim's organization.

How does it work?

The attack is launched when a guest attempts to log into the hotel WiFi. As part of the standard WiFi login process, the guests enter their last names and room numbers. The attackers know who is booked, so they can recognize their targets at this point, and only the targeted guests are then attacked.

Spyware secretly observes a user's activity, collecting sensitive information.

Keylogger

What is a keylogger?

A keylogger is a form of spyware that records all the user's keystrokes on the keyboard, including things that are copied/pasted from the keyboard, typically storing the gathered information and sending it to the attacker.

Olympic Vision

An example of a keylogger is Olympic Vision. This is a keylogger that can record keystrokes, record and steal data from the clipboard, take screenshots, and extract passwords from the web browser.

How does it work?

The keylogger would disguise itself in an email that is crafted to look like they're coming from a business partner or another company employee, also called Business Email Compromise (BEC) scams.

Each email had a file attached with the keylogger, Olympic Vision, which would then execute, collect data, and send it to the attacker.

What was the outcome?

This attacked 18 companies in the U.S., Middle East and Asia. In 2015, Business Email Compromise (BEC) schemes have caused a significant amount of damage to enterprises, amassing at least $800 million in total losses.

Olympic Vision caused $800+ million in losses.

Ransomware

What is ransomware?

Ransomware is a form of malware that locks you out of your device and/or encrypts your files, then forces you to pay a ransom to get them back.

WannaCry

In May 2017, a worldwide cyberattack called WannaCry targeted computers running the Microsoft Windows operating system by encrypting the hard drive, making them impossible for users to access, and demanding ransom payments.

How does it work?

WannaCry exploited a critical vulnerability in Window's Server Message Block (SMB) protocol; a transfer protocol used to transfer files between computers.

What was the outcome?

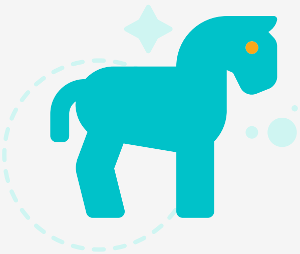
The attack was estimated to have affected more than 200,000 computers across 150 countries, with total damages ranging from hundreds of millions to billions of dollars.

WannaCry caused billions of dollars in damages.

Trojan

What is trojan?

Similar to Greek mythology, Trojans present themselves as harmless, useful gifts, to persuade users to install them. Thus, Trojans typically appear as regular software, allowing unauthorized access to your computer.



Zeus

Zeus is a powerful trojan horse most commonly used to steal sensitive information, such as banking details. The malware can infect all versions of Microsoft Windows, and configured to steal virtually any information hackers want. Even to install ransomware on computers.

How does it work?

There are two ways for Zeus to get onto a computer. Either by downloading a file in spam emails, or a drive-by download.

Drive-by downloads happen when the hackers can corrupt legitimate websites, inserting their malicious code into that website, and then installs itself when the user downloads and installs a benign program.

What was the outcome?

Zeus infected 3.6 million computers in 2009, compromised more than 74,000 FTP accounts on such important networks as those of NASA, ABC, Oracle, Cisco, Amazon, and Bank of America, and stole and blocked information from the United States Department of Transportation, among other government agencies.

Malware Prevention

How do we prevent malware?

Now that we've gone over the different types of malware and how it can get into our systems, let's talk about how we can prevent malware from getting in.

Third-Party applications

Being mindful of where the download source is coming from is a good step in the right direction when it comes to securing devices. For example, downloading applications from the company-owned website is safer than downloading it from a third-party and plays a huge part in keeping our devices safe.

Emails

As for emails, we'll go more into this in the next chapter when we talk about Social Engineering, but a good rule of thumb is to be extremelly cautious when it comes to clicking links inside emails. Sometimes email links can be disguised as malicious software downloading to your computer or provoke us to provide sensitive information.

Either way, if you're not 1000% sure that the email was meant to be sent, then don't click on it!

Update, update, update

When it comes to applications or operating systems, the developers do a great job of keeping the programs they build up-to-date. Updates help resolve any bugs, increase security, and provide us with the best performance. As such, we should be in the habit of updating our software and applications as frequently as they are released.

Here are a few simple rhymes to help you pay extra attention to Malware Prevention:

- **Downloading an application? First check for company verification!**
- **When it doubt, throw it out!**
- **Don't wait, update!**

You've completed this section!

Awesome! You've now completed the Malware section. We hope the information that was shared in this section provides you with some tricks up your sleeve so that you can prevent malware attacks moving forward.

Safe Internet Usage

Getting started

As we go through this section, try and answer the following questions to familiarize yourself with what is considered to be safe web browsing. Knowing the why's and the what's will help put our minds at ease when browsing the internet, and keep our devices safe from harm.

- **Why is practicing safe internet usage important?**
- **What are the 10 different ways we can stay safe online?**

Practicing safe internet usage

We spend a lot of our time on the internet, from staying connected to our family and friends to browsing the web, the majority of what we do requires internet access.

As such, it's always a good habit to practice safe internet usage, so here's our 10 tips for keeping your devices secure from malicious or harmful attacks.

Did you know that the average person spends 3 hours and 15 minutes a day on their phones?

Study by Rescue Time (Sample size: 11k)

- **DO keep your wifi secure.** The majority of internet companies provide you with equipment (modem and built-in router), preset credentials, and basic configurations so that you can access the internet. As such, we recommend going through these top tips to further secure your wifi network: Keep your home Wi-Fi safe in 7 simple steps.

- **DO enter data only on secure websites.** Some websites that start with "http" and some are "https." HTTPS indicates that a website is secure and uses encryption to scramble your data so it can't be read. So if you're browsing the internet, beware of entering data on an http site.

- **DO use long and randomized passwords.** I know that we've already touched on this, but it's so important that it needs to be mentioned again. The stronger the password, the harder it is for someone to gain access to a person's account.

- **DO be wary of online "friends."** People you meet online are not always who they claim to be. Fake social media profiles are a popular way for hackers to cozy up to unwary users. Be as cautious and sensible in your online social life as you would be in person.

- **DO be cautious while in public places.** Public WiFi can be a target for hackers, so be mindful of the data you access on a public network, and don't forget that it's easy to peer over your shoulder while you're browsing websites too!

- **DON'T be an oversharer online.** Be sure not to post any sensitive information or anything that could be considered valuable information for cybercriminals (i.e. credit card information, home address, etc.).

- **DON'T get suckered by a good deal.** When we're browsing the internet, we want to be careful of where we are clicking. "Free" offers could be tactics designed for us to click on a dangerous link. If it's too good to be true, it probably is.

- **DON'T put off updating your computer.** Software updates ensure that we have the latest security patches. If possible, turn on automatic updates for third-party applications and ensure that you are updating your operating system as soon as they're released.

- **DON'T install unknown applications.** One of the goals for cybercriminals is to trick you into downloading malware. This malware can be disguised as a "trusted" application. To be on the safe side, only download applications from websites that you trust.

- **DON'T click on links in unknown emails.** One of the most common ways malware is distributed is through your emails. Be suspicious of any unsolicited offers, double-check URLs and file extensions. If you're not sure, then don't click on it.

You've completed this section!

You've finished our safe internet usage section! Now that you've gone through our top 10 tips, we hope that it leaves you with a few tricks up your sleeve to keep yourself safe when it comes to browsing the internet.

Social Engineering

Getting Started

As we go through this section, try and answer the following questions to familiarize yourself with social engineering:

- **What is social engineering?**
- **What is an example of social engineering?**
- **How can we protect each other from social engineering attacks?**

What is Social Engineering?

Social engineering is the art of using human psychology, rather than technical hacking techniques, to gain access to buildings, systems or data.

For example, instead of trying to find a software vulnerability, a social engineer might call an employee and pose as an IT support person, trying to trick the employee into divulging his password.

Social engineeirng is one of the most common attack forms, so we need to have full confidence in knowing how we can protect each other and ourselves from these types of attacks.

As we go through this section, we're going to learn one of the most common types of social engineering techniques, phishing.

Phishing

Phishing is a social engineering technique that's often in a form of a disguise and a clever way for someone to gain sensitive information such as usernames, passwords, and credit card data—without you knowing!

There are many types of phishing scams and attacks: email phishing, vishing, smishing, spear phishing, domain spoofing, and CEO fraud.

In the next few moments, we'll be going over a few types of phishing scenarios and what to look out for to keep everyone's data secure and protected.

Story Time

An example of a successful phishing attempt was done in 2016. John Podesta (Hillary Clinton’s Campaign Chairman) received an email from “Google,” requesting that he change his password.

He then went to the IT Team, who suggested that he reset his password, and provided a Google link to have him reset his password.

Instead of using that link, he clicked on the “Google” link in the email and provided the previous password that was used. By doing so, **it gave a Russian cyber-spying group, Fancy Bear, access to John Podesta’s email account.**

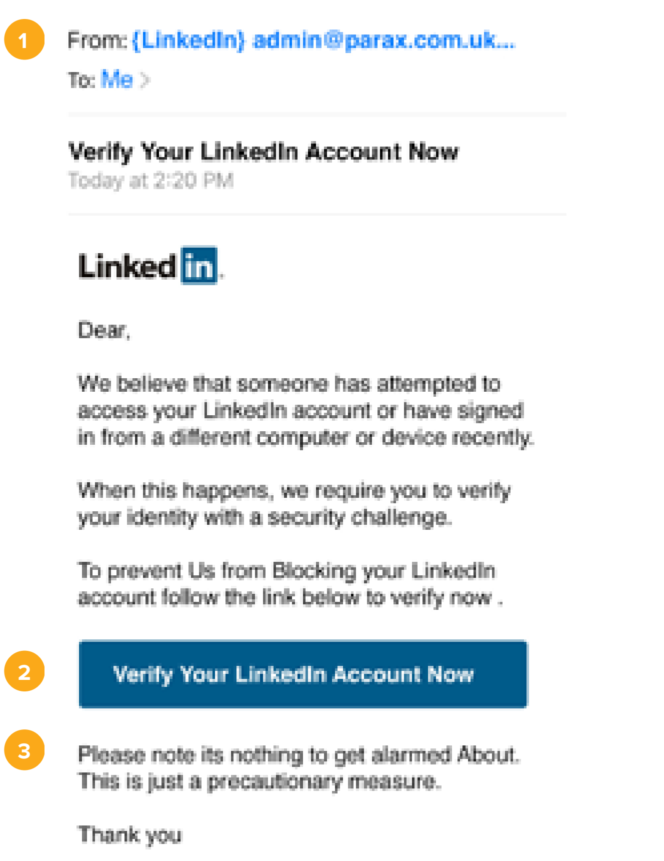
Story Recap

As you can see, even though emails may appear to look authentic, they might not be. Cybercriminals are only getting smarter (and so are we). These emails are intentionally designed to trick you—and they can be pretty good at it too.

If ever you’re unsure whether or not an email is a phishing email, it’s always safer to reach out to the company who sent you the email directly. Other than that, here are a few helpful tips to help you spot a phishing email.

Activity: Spot the Fake

Here's an example of a phishing email. Let's go through it together so that we can get a better understanding of what a phishing email looks like (and what not to do) so that we can avoid it at all times.



From: {LinkedIn} admin@parax.com.uk...
To: Me >

Verify Your LinkedIn Account Now
Today at 2:20 PM

LinkedIn

Dear,

We believe that someone has attempted to access your LinkedIn account or have signed in from a different computer or device recently.

When this happens, we require you to verify your identity with a security challenge.

To prevent Us from Blocking your LinkedIn account follow the link below to verify now .

Verify Your LinkedIn Account Now

Please note its nothing to get alarmed About. This is just a precautionary measure.

Thank you

Make special note of the following, and the questions we should be asking ourselves:

1. **Email address:** Is this an email address from a known sender?
2. **"Verify Your LinkedIn Account Now" Button:** Hmmm, that's strange. Do I need to verify my LinkedIn Account?
3. **Language used:** Is the email free of punctuation and grammatical errors?

Forms of phishing

Now that we've learned about email phishing, there are two others that are quite similar: vishing and smishing.

Vishing

Vishing is a form of phishing, but this is when the cybercriminal reaches you by phone in order to retrieve sensitive information from you.

They might talk with a sense of urgency or act like they're a "manager" and ask for sensitive information from you. Whatever the case, don't feel obligated to provide them with sensitive information.

If you're unsure or don't feel comfortable, don't provide them with information and hang up!!

Smishing

Can you guess what smishing is? It's the text version of phishing. In this form, a text message would maybe display a "free credit" back to your phone plan or suspicious activity in your bank account.

Either way, same as emails, don't click on the link! If you're unsure, contact the company directly to see if the text message is authentic or not.

You've completed this section!

As you can see, there are many different ways someone can use social engineering techniques to gain information.

Privacy Legislations and Jane

Getting Started

In this section, we will be learning more about the different types of Privacy Legislations and how it relates to Jane. There is a lot of information here, and we don't expect you to know every single law under each legislation. However, understanding the basics is important when it comes to providing care to your clients.

By the end of this lesson, you should know how to answer the following questions:

1. **What is a Privacy Legislation?**
2. **Why does Privacy Legislations apply to Jane?**
3. **What is the difference between HIPAA and GDPR?**
4. **Who is the custodian of data?**

Answer Key

1. **Privacy legislation** falls under each country's respective privacy law and relates to the storing, and using of personally identifiable information, personal healthcare information, and financial information of individuals, which can be collected by governments, public or **private organisations**, or other individuals. They are in place to promote and protect the privacy of individuals.

2. **Jane is a tool used to help allied health care practitioners** run their business, so we are required to follow privacy legislation. Read more within each section titled, "Where does Jane fit into all this?".

3. **HIPAA is a United States law** that requires organizations that store Personal Health Information (PHI) to follow security and data privacy regulations, in order to keep clients' medical information safe. **GDPR is a European privacy and security law** that applies to organizations anywhere, so long as they target or collect data related to people in Europe.

4. **The Account Owner** owns the data entered into Jane, as they're responsible for gathering consent to store the data. They are considered the "**custodian**" of the data and Jane is the "data processor". This is set when the Jane account is first opened.

HIPAA

What does HIPAA stand for?

Health Insurance Portability and Accountability Act.

HIPAA
COMPLIANT

What is HIPAA?

This is a United States law that requires organizations that store Personal Health Information (PHI) to follow security and data privacy regulations, in order to keep clients' medical information safe.

What is considered Personal Health Information? Any information that concerns health status, the provision of healthcare, or payment for healthcare linked to an individual.

Who does it apply to?

It applies to healthcare providers, healthcare clearinghouses, and health insurance plans-- they are considered a "covered entity."

Where does Jane fit into all this?

A covered entity may choose to use a "business associate" to carry out its health care activities and functions, and that's Jane!

Since Jane is a tool used to help allied health care practitioners run their business, we have followed HIPAA's Security Rule that deals with the protection of electronically stored and transmitted health records.

Is Jane HIPAA compliant?

Yes we are. We've implemented processes to ensure that Jane is HIPAA-compliant.

Here is the security processes mentioned above that we've implemented that follow HIPAA's Security Rule:

HIPAA

Here are the security processes mentioned above that we've implemented that follow HIPAA's Security Rule:

Administrative Safeguards: We have a strict policy that we only access a Jane account when they need assistance from us.

Physical Safeguards: Jane utilizes state of the art data centers, complete with the latest security and surveillance technologies.

Technical Safeguards: Data that is entered into Jane uses 256-bit encryption, the same that banks use.

If you'd like to learn more about HIPAA and the Privacy Law in the United States, click here.

PIPEDA

What does PIPEDA stand for?

Personal Information Protection and Electronic Documents Act.

What is PIPEDA?

This is a Canadian law relating to data privacy. It governs how private sector organizations collect, use and disclose personal information in the course of commercial business.

Some provinces have their own set of separate privacy laws. For example, British Columbia, Alberta, and Quebec have their separate private-sector laws that are similar to PIPEDA. So if the organization doesn't interact with other provinces, the above provinces will follow their version instead.

Who does it apply to?

As mentioned above, it applies to private sector organizations. It also applies to federally-regulated businesses operating in Canada--they're considered the "organization" in PIPEDA's terms.

PIPEDA applies to organizations that engage in commercial, for-profit activities.

Municipalities, universities, schools, and hospitals are generally covered by provincial laws so PIPEDA may only apply in certain situations. For example, if a university is engaged in a commercial activity, like selling an alumni list, then PIPEDA will apply.

Where does Jane fit into all this?

Since Jane is a tool that clinics use to store personal health information, we work hard to ensure that we are following all of the privacy laws across Canada so that clinics can use Jane.

PIPEDA

Is Jane PIPEDA compliant?

Yes we are.

If you'd like to learn more about how Jane can help you be PIPEDA compliant, **click here.**

GDPR

What does GDPR stand for?

GDPR
COMPLIANT

General Data Protection Regulation.

What is GDPR?

This is a European privacy and security law that applies to organizations anywhere, so long as they target or collect data related to people in the Europe.

Who does it apply to?

It applies to a company or entity which processes personal data inside or outside of Europe, regardless of where the data is processed or a company is established. They are considered the “controller”, “data custodian”, or in Jane’s terms--the Account Owner.

Where does Jane fit into all this?

Since you are considered the “controller” of data, Jane is the “processor.” Meaning we process the data on your behalf.

Since we process your data, we also need to ensure that we are GDPR-compliant.

Is Jane GDPR compliant?

Yes! Not only are we HIPAA and PIPEDA compliant, we are also GDPR compliant as well.

In fact, we’ve implemented security procedures to ensure that clinics meet GDPR requirements. Here are a few things that we’ve done to help with that:

- Jane data for EU customers are stored in London, UK.
- Jane offers an Activity Log report to Account Owners so that they can see a detailed breakdown of all user activity.
- Account owners control permissions for each user, including patient charts, billing records, and schedule records.

End

jane.app

CERTIFICATE OF COMPLETION

Jane's Security and Awareness Training

Alison Taylor
Co-founder & CEO
jane.app

Trevor Johnston
Co-founder & CEO
jane.app

Congratulations! You've just completed Jane's Security and Awareness Training.

Remember, we are all considered the first line of defence when it comes to protecting any and all data, so we all need to take the initiative to understand what we can do to keep each other safe.

Thank You!