TERRANOVA SECURITY

Data Privacy Week: 6 Best Practices for Your End Users

How much do your employees know about data privacy?

The reality is most employees aren't aware of how their personal information is collected and used by most modern organizations. That said, with Data Privacy Week 2022 fast approaching, there's no better opportunity to learn more about this topic.

Data Privacy Week is designed to raise awareness about online privacy and educate individuals on protecting their personal information. The event also encourages organizations to be more transparent about how and why they collect customer data.

From January 24th to the 28th, professionals across Canada, the United States, and many counties across the globe can participate in online initiatives connected with this awareness event by sharing knowledge related to essential data privacy awareness best practices.

Enjoy these important data privacy tips you can easily share with your team members, remote colleagues, family, and friends to help them protect their data from phishing, social engineering, and other types of cyber attacks in 2022.

What is Data Privacy?

Data privacy refers to the extent to which an end user's sensitive data is shared with third parties online. Sensitive data can include (but is not limited to) an individual's name, address, date of birth, race, gender, contact information, credit card number, photograph, ID card number, IP address, or location data.

Essentially, sensitive data constitutes any data connected to real-world or online conduct, whether that's a financial transaction on an eCommerce site or an engagement (e.g., a like or share) with a social media post.

Why is Data Privacy and Data Privacy Week 2022 Important?

In many countries, data privacy is positioned as a fundamental right, one upheld by strict regulations. One of the best-known is the European Union's General Data Protection Regulation (GDPR), which details the rights of EU data subjects.

From the perspective of an individual or consumer, data privacy regulations are a vital component in safeguarding against unauthorized access to sensitive data by third-party advertisers to cyber criminals.

Data privacy is equally important for building trust with global customers based on processing, storing, and sharing their information. If this data isn't secured, not only is an organization putting its customer's details at risk of a data breach, it's also opening up the door to regulatory liabilities and fines.

Therefore, taking part in Data Privacy Week 2022 is crucial because it provides organizations and employees with an opportunity to rethink their approach to data privacy. It's also a means to discover new ways to implement protections against unwanted use or disclosure.

6 Data Privacy Best Practices to Show End Users in 2022

To help your employees keep sensitive information secure at all times, here are six data privacy best practices you can teach them during Data Privacy Week 2022. Each best practice supports strong information security in both their personal and professional lives.

1. Know what is considered personal information

Personal information is any information that can be used independently or with other information to identify an individual. This umbrella encompasses:

- Name, address, and date of birth,
- Passport or driver's license number
- Medical, criminal, or financial history
- Ethnic or racial origins
- IP address, if it can be traced to an individual
- DNA, fingerprints, and voiceprints

To protect this information, you should only share these and any other types of personal information when absolutely necessary and only with recipients you know and trust.

2. Beware of phishing attempts

Phishing emails are one of the most significant threats to your employee's personal information in 2022. Cyber criminals will use them to trick individuals into clicking on a suspect link or downloading a malicious file to steal their data, install malware to their device, and more.

To defend against these manipulative emails, you must:

- Avoid opening emails from unknown senders. If you're unsure if a sender is legitimate, you can always reach out to them over the phone to investigate further.
- Never click on links in unsolicited emails, as these can take you to a phishing website or download malware to your device.
- Don't respond to emails asking you to provide confidential or personal data. No reputable organization will ask for personal information by email.
- If something sounds too good to be true, it probably is, so ignore any emails proclaiming that you've won a prize or are eligible to receive a special discount.

3. Watch out for vishing and smishing attempts

Emails aren't the only medium that cyber criminals use to try and trick victims into handing over their personal information. Fraudsters will also use SMS messages and voice messages to trick users into giving up personal information.

For instance, an attacker might send an SMS message to an individual saying their payment details are about to expire, with a link prompting them to update them. Then if the user clicks on the link, they'll be taken to a phishing website where the attacker harvests their details.

Employees can counter vishing and smishing attempts by never handing out personal information over the phone and never clicking on links included in unsolicited SMS messages.

4. Report any email scams you encounter

If you encounter a phishing scam in your email inbox, don't just ignore it; report it. Reporting the email to your IT department, IT provider, or another governing body can help prevent the fraudster from scamming other users.

Most personal and enterprise-grade email solutions like Outlook, Gmail, and Yahoo give users an inbuilt option to report email scams.

However, it's worth noting that most countries also have a board that deals with phishing scams, which you can contact via email to report scams. Some of these boards include:

- In the United States: the Cyber Security and Infrastructure Agency
- In Canada: the Canadian Anti-Fraud Centre
- In the United Kingdom: the National Fraud and Cyber Crime Reporting Centre

Contact your IT department or local law enforcement to inquire further about the appropriate organization to contact in your region.

5. Take steps to secure your online shopping

While online shopping is a massive part of many people's day-to-day lives, it's also a prime target for cyber criminals. This reality means it's vital to take extra steps to protect your data when using an eCommerce site or third-party transaction platform.

You can make your online shopping experience safer by taking the following actions:

- Make sure the site is legitimate. The first thing you should do when shopping at a new ecommerce site is to check its legitimacy by doing the following:
  - Check the URL, making sure it begins with "HTTPS," showing that there is an encrypted communication between your browser, and checking the website has a closed padlock that indicates a secure transaction.
  - Look at the site's security certificate – In some browsers, you can click on the lock icon and a "Show Certificate" option to view who the certificate was issued by and when it expires.
  - Watch out for seals of approval from third-party security vendors
- Beware of identity theft and related fraud. In 2020 alone, the FTC had 4,720,743 fraud and identity theft reports, which means users need to be prepared to spot scams independently.
- Use multi-factor authentication wherever you can. Many online stores will ask you to create an account before checkout. If you do, create a strong password and set up multi-factor authentication if it's offered.

6. Don't use public Wi-Fi

Using public Wi-Fi to shop online may be convenient for making impulse buys and emergency purchases. Still, it can put your information at risk, as hackers can snoop on data transmitted throughout the network. That means you should never transmit your address and credit card information on a public Wi-Fi connection.

If you absolutely must shop online while connected to a public Wi-Fi access point, use a Virtual Private Network (VPN) to protect your data in transit so that it can't be tracked and harvested by cyber criminals.

Building a cyber-secure corporate culture during Data Privacy Week 2022

Regardless of industry, size, or location, any organization can become a target for cyber criminals. As a result, you need to focus on building a human-centric, cyber-secure corporate culture if you want to safeguard your organization's data.

Data Privacy Week is the perfect opportunity to kickstart a year-round focus on data privacy and security awareness. Educate your employees about the latest security best practices that they can use to stay safe whether they're working in the office or shopping from home.

You can use our free Data Privacy Awareness Kit to launch your data privacy awareness program. It includes a free interactive course and actionable guidance you can use to build cyber champions who can lead by example and help improve your employee's security awareness.

It's important to note that while Data Privacy Week 2022 is a critical time for raising data privacy awareness, that doesn't mean you should stop the conversation on the 29th. Data privacy Week is best used as an opportunity to start building a security awareness program and communicating about cyber threats year-round.

If you want to dive deeper into data privacy, you can use these National Cybersecurity Alliance Data Privacy Week resources to find out more:

- Get Involved in Data Privacy Week
- Manage Your Privacy Settings
- Become a Data Privacy Week Champion
- Learning About Data Privacy

As measures like the GDPR and the California Consumer Protection Act (CCPA) raised awareness over the need for data privacy, more and more consumers realize how large corporations are leveraging and sometimes exploiting their personal information.

While these laws have created a lot of publicity, many people still don't fully understand them and impact their rights. You can find more information on how your organization can upload data privacy best practices from these Terranova Security GDPR and CCPA resources.

Recap

Talking openly about data privacy is the first step to building a security-aware culture. The better employees understand how websites and companies use their data, the more careful they will be about sharing their sensitive information online.

By bringing data privacy concerns to top-of-mind during Data Privacy Week 2022, you can help employees learn how to protect their private information and think twice before agreeing to share their personal data.