Data Privacy Day 2020: Learn 6 Easy Data Privacy Awareness Best Practices

Data Privacy Day is happening on January 28th in Canada, the United States, and many other countries. This day is important in highlighting the impacts technology has on day-to-day living and working. It's also a great opportunity to help your workforce learn new data privacy awareness best practices.

Unfortunately, while so many people are digitally connected and mobile, most people are unaware of the importance of protecting their data privacy and security. The goal with Data Privacy Day is to get people thinking and talking about data privacy at home, work, and on-the-go.

Protect your employees/coworkers, family and friends from privacy breaches and identity theft. Share these five tips to help them recognize phishing, social engineering and other cyber-attacks.

6 data privacy awareness tips for your users:

1. Know what is considered personal information

Personal information is defined as information that can be used on its own or with other information to identify an individual. Examples include a person's:

- 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

2. Beware of phishing attempts

The goal is to trick email recipients into any number of actions, ranging from the traditional phishing action of “click this link,” which results in a malware installation on your machine, to asking you to share more personal information for the purpose of extortion.

Remind your users of these email best practices:

- If you don’t know who sent the email, don’t open it. If you do know where the email came from, but it seems a little strange, exercise caution. Ask yourself a few questions: do I typically communicate with this person via email? If so, would he email me at this time of day? And if you’re still in doubt – call him!
- Don’t click on links in unsolicited emails. Period.
- Never reveal confidential information in an email.
- If a deal sounds too good to be true, it probably is.

3. Don’t be duped by phishing’s cousins, vishing and SMiShing

Other social engineering methods to get you to give up personal information, call or contact an organization or person via phone, or install malware by clicking a link or opening a file come at you via text message (SMiShing), phone (vishing), or social media platforms that have been compromised. These fraudulent communications can appear to be coming from the government (IRS, Census Bureau or law enforcement), or from someone you know whose account has been compromised. For example, a successful vishing campaign that senior citizens should be aware of is a phone call from a grandchild asking for money.

And remember, the guidance above holds true if you receive unusual communications via text, phone or social media.

4. Report email scams

Whether it’s to your IT department, email provider or to a governing body, make sure you have enabled the report phishing button and be proactive against phishing (even in your personal inbox).
Most email providers have built-in mechanisms that make it easy to report an email scam. The report phishing button can be enabled in Outlook, Gmail, Yahoo! and other email clients.

You should also know that most countries have a governing body that deals with phishing email scams. In the United States, the email can be sent to the Cyber Security and Infrastructure Agency. In Canada, report the email to the Canadian Anti-Fraud Centre. In the United Kingdom, email scams can be reported to the National Fraud and Cyber Crime Reporting Centre.

5. Remember these few key points when you shop online

- Validate that the site is legitimate. If you’re shopping at a new site you’re not familiar with, it’s worth checking its legitimacy. You can do this using a few methods:

    - Check the URL, paying close attention to domains and subdomains and ensuring it begins with “https://.” The “s” indicates an encrypted communication between you (your browser) and the website. A closed padlock also indicates a secure transaction.
    - Dig in and find the details of the certificate.
    - Watch for seals of approval from third parties such as security vendors.
- Identity fraud is growing. According to a study released last year from Javelin Strategy and Research, identity thieves stole $16.8 billion from U.S. consumers in 2017. The study also showed online shopping fraud (where the physical card is not present) is 81 percent more likely than point of sale fraud, as the use of chip cards and EMV® (Europay, Mastercard and Visa) payment grew in the U.S.
- Use multi-factor authentication wherever you can when shopping online. Many online stores will ask you to create an account with them as you check out. If you do (rather than check out as a guest), make sure the password you create is strong. Better still, use multi-factor authentication if it’s offered. And even though you’re encouraged to save your payment information on the site, the convenience of doing so may not be worth the risk if you’re not a frequent shopper of the site.

6. Don’t use public Wi-Fi

You may be tempted to use open Wi-Fi networks to shop online. Whether it’s online impulse shopping or simply using in-store Wi-Fi to save time, don’t trust your address, credit card information and anything else personal to public Wi-Fi.

Focus on building a cybersecure corporate culture

Every company regardless of industry, size, and location is a target for cyber criminals. This means that you need to put a focus on building a cybersecure corporate culture.
January 28th is an ideal day for companies to kickstart a year-round focus on data privacy and security awareness. Take advantage of the Data Privacy Awareness Kit to launch your data privacy awareness program. This kit gives you access to a free interactive course and a variety of communication tools, helping you to build cyber champions who can lead by example, keeping the data privacy dialog going year-round.

While January 28th is a critical day in raising awareness of data privacy – we don’t want the conversation to stop on January 29th. Interesting and engaging data privacy awareness training, simulations, and communication keep the conversation going year-round.

You can also take advantage of these NCSA Data Privacy Day resources to keep people talking and thinking about data privacy:

- Get Involved in Data Privacy Day
- Update Your Privacy Settings
- Become A Data Privacy Day Champion

Learning About Data Privacy

Measures such as GDPR and the California Consumer Protection Act (CCPA) are helping to raise awareness of the need for data privacy. More and more people are realizing how their digital footprint is being used by large corporations.

While the GDPR and CCPA have created substantial online buzz, many people simply do not understand how these policies impact them:

GDPR

This European Union (EU) policy gives people a “bill of rights” for protecting their data. This set of rules gives EU citizens control over how their personal data is used by companies operating in the EU. The GDPR applies to any company operating in the EU or that provides products and services to EU citizens. Admittedly, the GDPR policy is not simple or straight-forward. Use this free GDPR trial to raise awareness of GDPR in your company.

CCPA

This California-based policy requires organizations to give their California customers easy access to how their data is being used and shared. This includes giving people the ability opt out of having their data shared with other organizations. The CCPA applies to any company operating in California that either has $25 million in annual revenue, collects data on more than 50,000 users, or earns more than 50% of its income from user data. This policy was established around two key consumer rights “the right to know” and “the right to say no”. To help your employees learn more about CCPA, give them these two links: California’s Privacy Law Goes Into Effect Today. Now What? and CCPA Fact Sheet.

It’s important that companies talk about data privacy as part of building a cyber security aware culture. When your employees understand how their data is being used by websites and companies, they are more likely to think twice about sharing their personal data and credentials online.

By putting data privacy front-of-mind, it’s much easier to get employees engaged with how and why cyber security awareness is important. This has a trickle-down effect of raising awareness on how important it is to think twice before agreeing to share personal data.