Newsletter

Celebrating 32 years serving Central, N.C. *February 2022*

Data Privacy: How to Take Back Control of Your Data

From social media to online shopping, our lives and the digital world have become more and more intertwined every day. And while the digital world has afforded us a whole new level of convenience and access to information, consumers must remember the best practices for protecting their data and ensuring it is used the right way.

By 2020, it was estimated that 1.7 MB of data was generated by every individual worldwide every second. This includes data about an individual's activities, behaviors, and interests. Data comes in many forms, personal data, like social security and driver's license numbers, and physical data, like health data. With all this digital activity and data flying around, it is easy for individuals to feel like they have lost control of their data.

Consumers are rightly becoming increasingly concerned with data privacy, with 86 percent of individuals saying that they care about their data privacy. That said, even the savviest digital users can have trouble managing their data.

Here are a few steps to better manage your personal information and make informed decisions about your data and its use:

Understand the Privacy/Convenience Tradeoff

Before you even use their services, many accounts ask for access to personal information, such as your geographic location, contacts list, and photo album. This personal information has tremendous value to businesses and allows some to offer you their services at little to no cost.

Make informed decisions about whether to share your data with certain businesses by considering the amount of personal information they are asking for and weighing it against the benefits you may receive in return. Be thoughtful about who gets that information and wary of apps or services that require access to information that is not needed or relevant for the services they are offering. Delete unused apps on your Internet-connected devices and keep all apps secure by performing updates.

Manage Your Privacy

Once you have decided to use an app or set up a new account, check the privacy and security settings on web services and apps and set them to your comfort level for information sharing. Of course, each device, application, or browser you use will have different features to limit how and with whom you share information. With so many different settings to manage, staying on top can be very challenging. However, here are a few important ones to focus on first:

Upcoming Events

Lunch & Learn:
Cyber Insurance with Marsh & McLennan Agency
February 10, 2022

Webinar:
Increasing Productivity in the Digital Workplace
February 23, 2022

For more information on our upcoming events, please visit www.tcsusa.com.

336.804.8449 I info@tcsusa.com I www.tcsusa.com

- Geolocation Data: Many apps will ask you to share your location data with them. Ensure that you are only sharing this data with apps you trust and that these apps are using your information responsibly. I tend to allow geolocation but only when using the app.

- Contacts Data: Email apps and video conferencing apps virtually all allow individuals to sync their existing contacts with their services automatically. Therefore, you must share this data only with trusted sources as not only is contact data yours, but it is your friend's and family's as well. I have made a practice of not doing this and have had no issues when video conferencing.

- Camera and Photo Data: Social apps universally ask for access to an individual's photo library and related camera data -- which contains troves of private information. Be sure only the most trusted sources have access to this information and double-check settings in the app to filter which photo files apps have access to.

You can find more information for free through great resources like the National Cybersecurity Alliances' Manage Your Privacy Settings page.

Protect Your Data

Data privacy and data security go hand in hand. And fortunately, there are numerous easy-to-implement steps that everyday individuals can take to shore up their data and general cybersecurity:

- Long, Unique Passwords: Thanks to automation, once a bad actor has compromised one password, they can quickly bounce it around other sites to access other accounts. Having long, strong, and unique passwords for each account immediately thwarts these "easy hacking" efforts and makes it much harder for hackers to crack a password in the first place.

- Password Managers: Password managers have redefined cybersecurity by providing a consolidated and secure hub for individuals to store their information. Password managers can even generate unique, secure passwords for you and keep them automatically.

- Multi-Factor Authentication (MFA): MFA has been found to block 99.9 percent of automated attacks when enabled and can ensure your data is protected, even in the event of a data breach. And the great news is, many organizations are increasingly offering it to individuals as an opt-in -- if not mandating it completely-- so it is easier than ever to enable.

76% of individuals said it's too hard to understand what is going on and how their information is used. However, by keeping these few quick tips in mind, individuals can keep much better tabs on their data and create a safer digital environment for themselves.

Changing the Passcode

We received a call recently from 'Law Firm' with some questions about their phone system and the fact that it was used to make international phone calls. The international charges they were being asked to pay were for calls that Law Firm employees had not made. Law Firm uses a popular phone system and their integrated voice mail system. The Law Firm asked TCS to investigate if hackers had possibly gained access to their network to take over their phone system. TCS found that the phone vendor had left the default passcode on the phone and voicemail system. By leaving the default passcodes on the system, they "effectively left the key under the front door mat" for anybody who wanted to gain access.

Please get in touch with your phone vendor and confirm that they have used a unique passcode for your telephone and voice mail system. This same problem could exist for your copier/printer/fax machine, alarm system, HVAC system, Wi-Fi, IP Cameras, etc.

Never leave the default passcode on any equipment at home or work, even if it is not connected to the Internet.

Getting Technical: How One Small Distribution Company Leveraged the Cloud

Tri-State Steel wanted to find a Cloud-based solution to improve their ability to meet customer needs and exceed their expectations. They wanted a solution that would give them the same functionality available to a large distribution company. With their AS400 IBM system, most processes were manual, and improvements were complex and burdensome. Tri-State's AS400 system had one person developing and supporting their software, which was a condition that would not help Tri-State to meet their goals.

Important to owner Steve Scott was the ability to work in real-time. "I needed to be able to run Tri-State Steel from anywhere at any time; customers did not need to be concerned [whether I was in or] out of the office for the day." If you could expand that to the whole company, you would have a very customer-centric environment, "which would enable us to deliver excellence." Scott was faced with questions such as, what would happen to Tri-State if they did not have their one-person support? How were they going to leverage technology to achieve their vision?

Scott recognized that to become a player in the global market; they would need to take certain steps to implement a solution that would allow them to be a competitor while continuing to operate as a small business.

Scott started with an industry software vendor and interviewed multiple system integrators to meet his need to find a best in class software system that would be used by larger steel companies. One of his concerns was to be able to expand his business through mergers and acquisitions. In this case, the application needed to be adaptable to changes within the steel industry. The software also needed to be affordable and scalable. As part of the decision process, it was imperative that the industry software vendor was able to work closely with the system integrator so that Tri-State could focus on running their business. "There was only one way to do this; the system integrator needed to understand and be able to work through what it was going to take to create an enterprise class solution."

Business continuity was at the core of this solution. Tri-State was worried about communication; they wanted a system that made it seamless. "The call you take from a customer may be the only time they have talked to a steel company today, even if that is your 999th call." Tri-State wants to make the customer feel like they are the most important person they talked to today. Therefore, once an order was placed over the phone, production and response were nearly instantaneous,and communication was enhanced. Tri-State has been able to continue this thinking even with increased volume, with the Cloud-based solution. What was a source of employee frustration is now more job satisfaction.

How TCS Helped

The application vendor chosen did not support server virtualization technology. TCS recognized this during the quoting stage of the project and consequently won the business as the only firm to recognize this important distinction. TCS engineered a solution for Tri-State that gave them the look and feel of a cloud solution while allowing the application to run on the dedicated hardware that the vendor required. Placing the solution in the TCS Datacenter gave Tri-State the Cloud Solution they desired with redundant Internet, redundant power and near line availability in the event of disaster. Along with cloud-enabling their new Industry Software ERP System, TCS helped Tri-State move their email to the cloud and allow their file storage to be Cloud-based as well, effectively giving Tri-State what is normally called "Hosted Infrastructure."

TCS setup the hosted infrastructure, the Remote Desktop environment that all users operated from and worked with the application vendor to install the software. TCS did all of this with very few interruptions to Tri-State's daily operations and on budget and within the time allotted. TCS succeeded in delivering a solution that will hold up over time.

Tri-State's modern-day solution helped them become efficient and significantly improve record keeping and data management. A cutting-edge company that knew what they wanted and partnered with a trusted IT service partner to deliver advanced technologically to meet their needs today and into the future.

Ben Pike

Analyst

ASK A TECHIE

"Is a VPN connection advised if using O365 for a remote user?"

Suppose you are working at your home or office. In that case, you do not need to be connected to a virtual private network (VPN) service provided by Private Internet Access or any others. However, our recommendation is if you are at a coffee shop, airport, hotel, or using any other public WiFi, you should connect to a VPN. The rule of thumb should be; is this network owned and managed by someone you know and trust? If yes, then you most likely do not need a VPN.

5601 New Garden Village Dr.
Greensboro, NC 27410

In this Issue

LUNCH & LEARN: Cyber Insurance with Marsh McLennan Agency

Date: Thursday, February 10th, 2022
Time: 12:00 PM
Speaker: Murphy Holderness, Business Insurance Consultant, MMA
Registration: Visit tcsusa.com/events/ or call 336.804.8449

Join us for an informational session with Marsh McLennan Agency as they discuss current cyber market trends and how they impact underwriting guidelines. These guidelines drive protocols that your organization must have to reduce exposure while securing the best coverage and pricing possible.

Organizations are still not doing enough to protect their data or recover from a breach. As a result, employers of all sizes still appear to be vulnerable to the risks of cyber-crime and data breaches. And now, there are many technology implications because of changing work environments.

To register, please visit www.tcsusa.com/events/