

IDENTITY AND PRIVACY

Why your data matters and how to protect it



THIS MONTH'S TOPICS:

Privacy vs. Convenience

Data Privacy Week...

Identity Theft

Identity Theft Awareness Week

Scam of the Month:

Tax Scams...

Cyber Zen Den:

Understanding your cyber identity...

With Data Privacy Week and Identity Theft Awareness Week, January is full of exciting celebrations in the cybersecurity world. To honor these cyber-based festivities, we're taking a closer look at these two major topics...

Though many assume that their data doesn't matter and that using the internet means giving up privacy, this notion can be quite harmful to our privacy and identity. While it is inevitable that some personal information will be offered up when online, there are still many ways to protect your personal information.

In this month's newsletter, find out why all personal data is valuable. Learn how data is collected and used, as well as how to spot and avoid identity theft.

PRIVACY VS. CONVENIENCE

In honor of January's Data Privacy Week:

HOW YOUR DATA IS ACCESSED

Any internet-connected device has the ability to collect data. Some websites, apps, and accounts ask for access to user data or use cookies. Others track emails or buy data. Data is also collected by search engines and social media platforms. Many companies access this data to sell it or to analyze consumers,



WHY DATA PRIVACY MATTERS

Many users just accept that their data is online. So why does it matter if advertisers use it to target ads? The truth is this data is used for much more. Often giving your phone number or email address leads to an influx of unwanted messages. Cybercriminals also benefit when user data is available online as it makes it easier to carry out scams or identity theft.



HOW TO CONTROL YOUR PRIVACY

- Manage privacy settings on every device. Whenever possible do not allow websites or apps to use your data.
- Use password managers and Virtual Private Networks (VPNs) to encrypt your connection and keep data safe.
- Always read privacy policies to understand what data is being collected and why.



TIPS FOR THE FUTURE

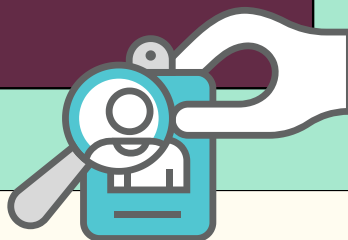
While it may be tempting to skirt privacy for the convenience of quick checkouts and logins, keep in mind the risks that these conveniences bring.

There is a tradeoff between convenience and privacy. For example, in order to get directions on your phone, the app will need to track your location. Understanding this balance will allow you to make an informed decision when dealing with data privacy in the future.



IDENTITY THEFT

IDENTITY THEFT AWARENESS WEEK: HOW TO SPOT AND AVOID IT.



Awareness Week

January celebrates Identity Theft Awareness Week, as a time to acknowledge the serious financial and social strain that many victims of identity theft experience. Learn how to protect your identity by understanding ways in which you can spot and avoid identity theft.

HOW DOES IT WORK?

Often starting with scams, cybercriminals gather personal information. Once they have enough, they begin opening accounts, filing taxes, opening credit cards, and carrying out other tasks under the user's name.



Spotting Identity Theft

Identity theft can be hard to detect as cybercriminals often change the user's address and notification settings. Some signs of identity theft include calls from debt collectors about purchases you did not make, unknown charges or withdrawals, or changes to your accounts, like no longer receiving bills or notifications.

Recovering from Identity Theft

1. Call the companies where identity theft occurred and get any unknown charges and accounts removed.
2. Check and correct credit reports.
3. Report if your Social Security number was used.
4. Place a fraud alert with a credit bureau.

HOW TO AVOID IDENTITY THEFT



Any documents with personal information such as health forms, billing statements, or expired credit cards should be cut up or shredded before disposal. Watch for phishing messages and stay up-to-date with cybersecurity best practices to avoid giving up additional personal information.

SCAM OF THE MONTH

Each month we highlight a scam that demonstrates tactics criminals are using RIGHT NOW, to better prepare you when the next scam hits.

Jonathan was going through his mail when he found a letter from the government. He opened it and was surprised when he read that more than one tax return was filed using his social security number. Though he had filed his tax return later in the season, he was sure he did not file twice.

Jonathan also received a notice stating that he received wages from somewhere he had never worked. He thought these notices were strange, but he figured they must have just been a mistake. Jonathan decided to ignore them and move on with his day.

What Jonathan didn't realize was that his personal information had been leaked in a data breach a few months prior, and a scammer had purchased his information on the Dark Web. This included his social security number, address, birth date, and more.

Since the scammer filed first, they were able to steal any refunds that Jonathan would have received.



Did you spot the red flags?

- ▶ Receiving a written notice that states more than one tax return has been filed is a red flag.
- ▶ Instead of calling to ask about the notices he received, Jonathan ignored them.
- ▶ Jonathan did not file his tax returns early, which gave scammers more time to file before him and take any money he would have received.



File taxes early. This will limit the time that a scammer can use your information. If you do receive any unusual notices, respond right away.



There are many different tax related scams that are carried out during tax season. Treat unsolicited text messages, emails, or threatening phone calls from tax service organizations with caution.



In some countries, you can use an Identity Protection PIN. This is an additional verification number that must be entered before filing tax returns. See what additional security options are available in your area.

Key Takeaways

While most people have some kind of personal information online, it is still important to protect that data and work towards data privacy.

There are many ways to recover from and prevent identity theft.



Prioritizing privacy over convenience:

Taking control of your privacy by deciding what companies and apps can access your data can help keep personal information secure.



Spotting and avoiding identity theft:

Know the signs to look for like account changes or unknown transactions. Avoiding phishing messages can also help protect your identity online.



Staying alert while doing taxes:

Filing taxes early and knowing how you will be contacted regarding your tax returns will help you avoid scams and stay on top of any potential fraud.

Self-identity

Being aware of your own identity and the unique potential and qualities that you possess in relation to the rest of society.

How does this relate to cybersecurity?

Some may think that their unique identity does not need to be protected online, but cybercriminals will take advantage by stealing the personal information of those who do not keep their identity protected.

Now apply this concept to cyber-awareness.

Think about your own identity and what unique information could be online about you that could be used by cybercriminals.

Use the tips in this newsletter to keep your information private and your identity safe.