THE PERSONAL SIDE OF SECURITY

How to keep your personal information safe online

THIS MONTH'S TOPICS:

Cyber Stories

The real impacts of fraud

The Future of Passwords

Is the future passwordless?

Scam of the Month:

Vacation Phone Scams...

Monthly Mashup:

Your Personal Privacy Quiz...

While the lessons and tips provided in cybersecurity training certainly are beneficial, understanding the personal side of cybersecurity is just as important.

It's easy to hear facts and statistics about a big breach, but what's harder is taking the time to truly think about how a cyber incident can impact us and those around us.

In this month's newsletter, read a personal story about the impacts of fraud, learn more about the future of passwords, and dive into the ways cybercriminals are capitalizing on your vacation plans. Don't forget to take the Personal Privacy Quiz to test your own social media privacy strength.

CYBER STORIES:

The Real Impacts of Fraud

For many, social media platforms are a part of daily life. However, their casual nature may lower guards when it comes to privacy. The story below shows the serious impacts of oversharing online.

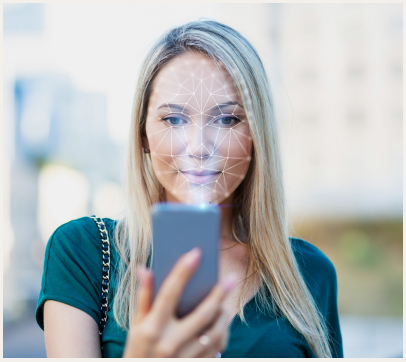
John is a hardworking businessman who is enthusiastic about growing his professional network. Social media and professional networking platforms seemed like just the place to do this. He interacts with new and old friends by posting about his daily activities, location, and vacations. John also updated his profile, so it shows his birthday and favorite places to shop. John joined a professional networking platform as well and added details about his past jobs, education, and favorite companies. John accepted all the friend requests that came his way and made sure his accounts were public so he could grow his network as much as possible. What John didn't know, was that this personal information was also accessible to and being monitored by cybercriminals.

Then, one day, John received an email that appeared to be from a legitimate company he follows. The message offered him a special deal for his birthday. John followed the link in the email and was directed to a website that looked nearly identical to the real company site. He entered his address and credit card number to receive the special birthday gift. What he didn't realize was that he had just handed over his sensitive data to cybercriminals. Now they had everything they needed to commit identity theft. Soon there were unauthorized charges in John's accounts, credit cards opened in his name, and loans he had not applied for. It took months for John to get the issues cleared up, and he suffered great financial and emotional tolls.

Tips to Avoid Oversharing:

- Analyze emails, even if they contain your personal details.
- Set accounts to private and only accept friend requests from those you know.
- Avoid sharing personal details on social media like birth date, location, or answers to security questions.

THE FUTURE OF PASSWORDS



PASSWORD

Definition: A combination of characters used to verify user identity before granting access.

Benefits: Simple to set up and the most common way to verify identity.

Drawbacks: If a password is not strong enough, it could easily be guessed or compromised.

MFA

Definition: Multi-factor authentication requires two or more verification methods before access is granted.

Benefits: Extra layer of security and harder to hack due to physical access and biometric factors.

Drawbacks: Requires an extra step for users. Often requires a second device.

PASSKEY

Definition: A passwordless method to verify identity through a private key stored on a device. For users, it's similar to unlocking a phone with biometrics or a PIN.

Benefits: Strong encryption, easy to use, and could limit phishing and breach success.

Drawbacks: Not available on all platforms or websites and still many unknowns.

IS THE FUTURE PASSWORDLESS?

While passwordless authentication is on the rise and has many benefits, as of now, passwords and multi-factor authentication still play a crucial role in security. Make sure you follow your company's preferred method of authentication when accessing accounts and devices.

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.

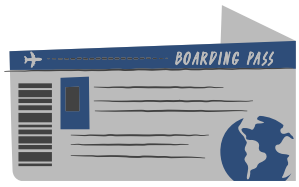
Sam had been saving up for a long-awaited vacation. Once it came time to book his flight, Sam searched the web for the airline's customer service number. He typed the number into his phone. When he called, an airline representative answered and helped Sam book his flight. All he had to do was give the representative some information about himself and his credit card details to book the flight.

A few days later, multiple unauthorized charges appeared on Sam's credit card statement. Sam reported the incident to the credit card company and the authorities. After retracing his steps, Sam realized he had misdialed the toll-free number for the airline by one number. The number he had dialed belonged to a scammer who purposely bought phone numbers close to those of well-known organizations. The scammer preyed on people who dialed the wrong number by pretending to be from the airline the person was trying to call.

Did you spot the red flags?

- Instead of searching for a phone number online, Sam should have gone directly to the company's website.
- Since Sam knew the airline he was trying to use, he could have clicked on the phone number in their app or on their official website to dial instead of typing it in.
- If unauthorized charges start appearing on statements, it is never a good sign. Sam took the correct steps by reporting these charges to the credit card company.

Many websites and apps allow you to click a phone number to call it, instead of typing it in. After verifying you are on the official website or app, consider this method to avoid mistyping.



Verify phone numbers after you type them in. Proceed with caution if anything seems off. If an airline asks for a wire transfer or gift card, hang up.

Travel-related scams come in many different forms. Verify websites and phone numbers before booking any hotels or flights. Research the company before booking through a third party. Travel with as few devices as necessary and make sure auto-connect is disabled for Wi-Fi and Bluetooth.

THE MONTHLY MASHUP

KEY TAKEAWAYS

The personal side of cybersecurity puts into perspective the extra time it takes to implement security best practices. By double-checking websites, phone numbers, and the information you post on social media, you can better protect yourself from the serious impacts of a cyber-attack.

YOUR PERSONAL PRIVACY QUIZ

How private are you? Take the quiz and check your answers to find out!

1. How often do you fill out fun challenges or quizzes on social media?
    a. Never
    b. Once or twice
    c. All the time

2. How many of your social media accounts are set to private?
    a. All of them
    b. Some of them
    c. None of them

3. What information have you shared on social media?
    a. Pictures of hobbies, family, or friends
    b. Your date of birth, address, or phone number
    c. Information from both of the above categories

4. What do you do if you receive a friend request from someone you don't know?
    a. Decline or ignore them
    b. Accept some of them
    c. Accept all friend requests

5. Are any of the answers to your security questions available in the information you share on social media?
    a. None of them
    b. Some of them
    c. All of them

How did you do?

Mostly A's: Privacy Pro! Keep up the good work!

Mostly B's or even mix: Pretty good privacy practices! Make sure your good privacy habits are consistent across all accounts.

Mostly C's: Practice makes perfect! To improve your privacy, try implementing the "A" answers to your social media accounts.