TRU Technical Partners
IT SUPPORT & CYBERSECURITY

Newsletter: April 2024

PII AND PASSWORDS

Examine the importance of protecting PII and using strong passwords

THIS MONTH'S TOPICS:

PII Journey

Follow PII on a journey across the web

Password Managers

A deep dive into password managers

Scam of the Month:

Remote Work Scams...

Monthly Cyber News:

April News and Upcoming Dates...

Personally Identifiable Information (PII) and passwords are important terms in cybersecurity. Think of each bit of PII as a puzzle piece that outlines who you are. Your password is the lock on the door that keeps the puzzle safe. The stronger the lock, the safer your puzzle pieces.

We're constantly sharing and accessing all sorts of PII. By using strong passwords, we're not just keeping our own details safe; we're also protecting the information that our customers and colleagues trust us with.

In this month's newsletter, explore the implications of PII getting into the wrong hands and improve your passwords with password managers.

JOURNEY OF PII

Follow PII on a journey across the web!

Stop 1 - Shopping Site

PII, including credit card information and email address, are entered onto a shopping website.

Stop 2 - Data Brokers

The shopping website shares customers' buying habits and data with third-party data brokers.

Stop 3 - Cybercriminal

The shopping website suffers a data breach and customer information is exposed.

Stop 4 - The Dark Web

The cybercriminal who breached the shopping website posts the PII on the Dark Web.

Stop 5 - Phishing Message

Phishing messages are sent to the exposed email addresses using other exposed PII to make them more convincing.

Stop 6 - User Updates

Passwords should be changed after a breach. Credit cards and email addresses might need to be changed, as well.

Stop 7 - Home!

Some PII returns back home in new forms (though the original PII is likely still on the Dark Web.)

Reminders

- Enter as little PII as possible on websites.
- Just because an email includes your PII, doesn't mean the message is legit.
- If you are notified of a breach, change exposed passwords, credit cards, and other PII if possible.

Password Managers

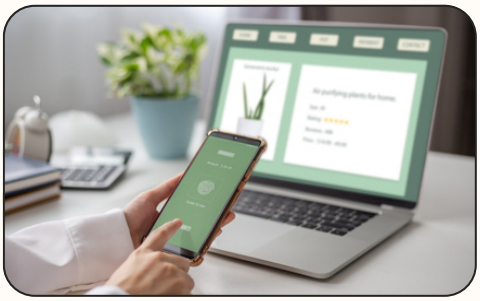
How do password managers work?

Password managers are designed to store and manage your online credentials. Typically, these tools encrypt your passwords and keep them secure with a master password that you create.

What are the risks?

With all of your login information in one place, the impacts are magnified if the password manager suffers a breach. Most password managers have security in place so if a breach does occur, the cybercriminal cannot access your passwords. Choose a password manager that has strong encryption practices and offers MFA. There is also the risk of losing passwords since many password managers do not offer recovery options for forgotten master passwords.

What are the benefits?



Generate Passwords:

Passwords managers generate new, complex passwords for you.

Improve Passwords:

Use longer, unique passwords for every account since password managers remember them for you.

Autofill information:

Many password managers autofill your login info into websites, increasing efficiency while staying secure.

Picking a Password Manager

Not all password managers are created equal. Look at the company's reputation, the security features offered (it should offer MFA for example), and whether it works across all platforms you use.

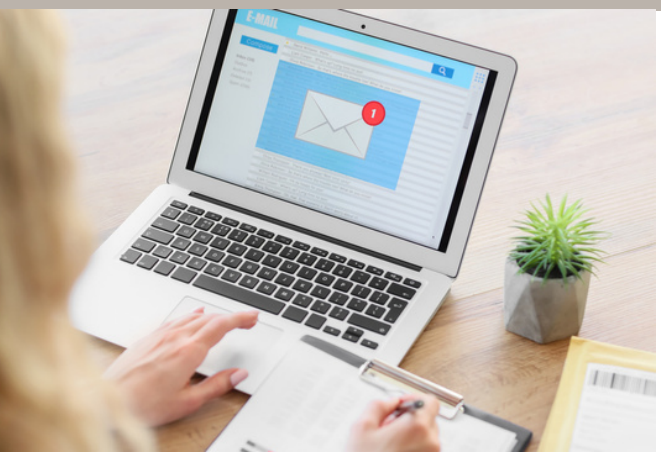
Check with your organization before picking a password manager for work accounts. For personal accounts, research and figure out which password manager fits your needs.

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.

Lily's company recently allowed her to transition to working remotely. She was excited to have the opportunity. One morning as she was settling into her new, remote office when she received an email from the IT department, detailing an update to the staff portal and asking her to log in to update her section. The email looked professional, complete with the company logo and a link to what appeared to be the company's login page.

Lily clicked the link and entered her credentials. Unfortunately, the message was from cybercriminals, and she inadvertently gave them access to her account. The cybercriminals quickly exploited this by attempting to continue the breach further into the company's network. They were successful and were able to send phishing emails to Lily's contacts, modify forwarding rules, and access sensitive company information, including finance-related communications with clients.



Did you spot the red flags?

- Lily should have checked if the sender's email address matched that of her company's IT provider.
- Lily should have verified the email with IT or her supervisor before clicking the link.
- Employees should proceed with caution when they receive an out of the blue request with no further explanation.

This scam is part of a broader trend exploiting the shift to remote work. Cybercriminals are leveraging this new terrain which might not have as established security practices. Remote workers should make sure to verify messages, just as they would in the office.

When working remotely, remember to follow cybersecurity best practices like avoiding public Wi-Fi, keeping work and personal files separate, and using strong passwords and multi-factor authentication.

CYBER NEWS

INCREASE IN DIGITAL WALLET SCAMS

Accidental deposit scams are on the rise. These scams occur when a cybercriminal "accidentally" sends money to a user's payment app like Zelle or Venmo. They then message the user, asking them to send the accidental payment back. If the user does interact with the scammer and send the money back, they might become part of the scammers money laundering scheme where they use these payment apps to take money from hacked bank accounts. Users should resolve these issues with the payment company's customer service instead of interacting with the potential scammer.

UPDATES & EVENTS

-May 2nd is World Password Day. To celebrate, update any passwords that aren't unique, complex, and long. Consider using a password manager.

VEHICLE SCAMS ON THE RISE

There has been a rise in fake vehicle listings online. Cybercriminals have been crafting fake listings and websites and presenting too-good-to-be-true deals that are hard to verify due to the supposed rarity of the vehicles. The cybercriminals may even include a fake vehicle history report to lend credibility to their listing. Avoid these scams by researching the seller, insisting on seeing the vehicle in person before buying, and proceeding with caution when asked to pay through unusual or untraceable methods.

Get it touch with us!
408.559.2800 | info@trutechnical.com
Visit us at www.trutechnical.com