precision
CYBERTECHNOLOGIES & DIGITAL SOLUTIONS LTD

CYBER DIGITAL WORLD

NEWSLETTER

Volume: 26 October 2023

For this issue of the newsletter, we will be focusing on the importance of password managers, and how does this positively or negatively impact your cybersecurity posture?

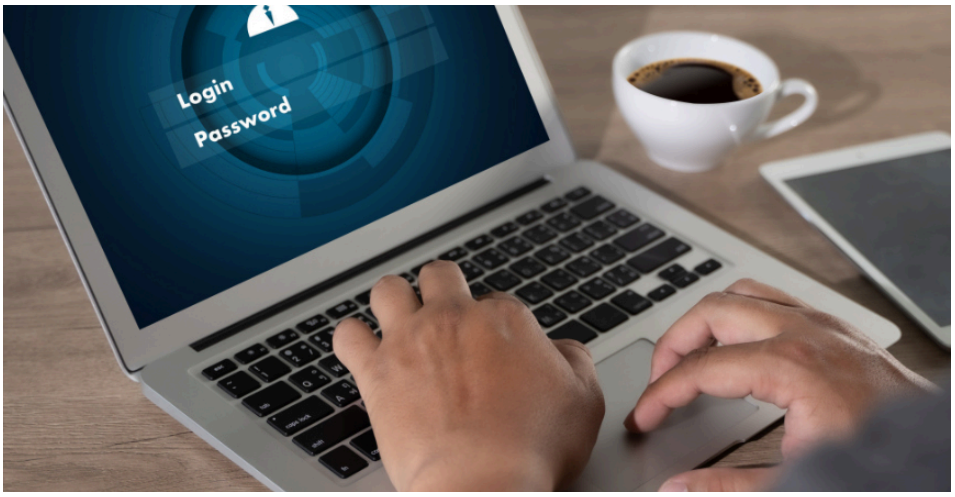
Dr. Ronald Walcott
Managing Director

INTRODUCTION

The digital realm is intimately tied to our everyday lives. Since our lives are knitted together with the digital realm where we have a vast amount of personally identifiable information (PII) stored digitally, it is incumbent upon us to safeguard this information to the best of our ability. Today we are going to focus on one of these ways we can protect our information, which is by utilizing Password Managers.

THE IMPORTANCE OF PASSWORD MANAGERS

These digital guardians serve as an essential tool in our ongoing battle against cyber threats, offering a convenient and secure solution to a problem that affects individuals, businesses, and organizations worldwide. As we navigate the vast expanse of the internet, safeguarding our personal information, financial assets, and digital identities has emerged as a paramount concern. This introduction delves into the pivotal role that password managers play in the modern digital landscape, shedding light on their significance in protecting our online lives, simplifying our digital routines, and bolstering our overall cybersecurity posture. From simplifying the complex web of passwords to fortifying the defenses against relentless cyber adversaries, the importance of password managers cannot be overstated.



WHY ARE PASSWORD MANAGERS IMPORTANT?

Password managers are crucial in the digital age for several compelling reasons:

1) **Enhanced Security:** Password managers generate and store strong, unique passwords for each of your online accounts. This reduces the risk of unauthorized access, as complex passwords are difficult for hackers to crack.

2) **Protection from Phishing:** They can recognize legitimate websites from phishing attempts, ensuring you don't inadvertently disclose your login credentials to fraudulent sites.

3) **Convenience:** Password managers simplify the process of logging into websites and apps. You only need to remember one strong master password to access

CONTINUED ON PAGE 2

In this Issue:

THE IMPORTANCE OF PASSWORD MANAGERS

HEADLINE NEWS:
HOW CHATGPT CAN HELP CRIMINALS GET THERE

UPCOMING EVENTS

all your stored passwords, streamlining your online experience.

4) **Encrypted Storage:** Password managers use strong encryption to store your credentials securely. Even if their databases were breached, it would be extremely difficult for attackers to decipher your passwords.

5) **Data Breach Alerts:** Some password managers offer breach monitoring services, alerting you if your login credentials are found in a known data breach so you can take immediate action.

WHAT ARE THE CONS OF USING A PASSWORD MANAGER?

While password managers offer numerous advantages, they also come with some potential drawbacks and considerations:

1. **Single Point of Failure:** Your master password is the key to all your stored passwords. If you forget it or it gets compromised, you may lose access to all your accounts.
2. **Initial Setup Complexity:** Setting up a password manager and migrating existing passwords can be time-consuming and initially confusing for some users.
3. **Cost:** Some premium password managers may require a subscription fee, although there are free options available.
4. **Security Concerns:** Although password managers are generally secure, they are not immune to vulnerabilities or breaches. You must choose a reputable and regularly updated password manager.
5. **Recovery Procedures:** In the event you forget your master password or lose access to your password manager, the recovery process can be complicated or, in some cases, impossible, because the data is encrypted with your master password.

In conclusion, while the use of a password manager can greatly enhance your online security and convenience, it's important to be aware of these potential downsides and take steps to mitigate them. Choosing a reputable password manager, maintaining strong master password practices, and keeping backups of crucial information are some of the ways to address these concerns and maximize the benefits of password management.

Frequently Asked Questions:

Here are five frequently asked questions about password managers:

1. IS IT SAFE TO STORE ALL MY PASSWORDS IN ONE PLACE WITH A PASSWORD MANAGER?

Users often wonder about the security of consolidating their passwords in one location. Password managers use strong encryption and security measures to protect your data.

2. WHAT HAPPENS IF I FORGET MY MASTER PASSWORD?

Losing your master password can be problematic since it's the key to your password manager. Some password managers offer recovery options, but they usually involve additional security measures.

3. ARE PASSWORD MANAGERS COMPATIBLE WITH ALL WEBSITES AND APPS?

Password managers are generally compatible with most websites and applications, but there may be occasional compatibility issues, especially with some less common or older platforms.

4. DO I STILL NEED TO REMEMBER ANY PASSWORDS IF I USE A PASSWORD MANAGER?

While a password manager can generate and store complex passwords for you, you still need to remember your master password. It's the one password you must commit to memory since it unlocks all your other passwords.

5. HOW DO I CHOOSE THE RIGHT PASSWORD MANAGER FOR MY NEEDS?

Users often inquire about the best password manager to suit their requirements. The choice depends on factors like the platform (Windows, Mac, Android, iOS), features (secure sharing, password strength analysis, multi-device support), and your budget.

These questions provide insight into common concerns and considerations when using password managers, helping users make informed decisions about their digital security practices.

Headline News

Phish Perfect: How ChatGPT Can Help Criminals Get There

ChatGPT can craft a near-perfect phishing emails in five minutes, nearly beating a social engineering team with decades of experience by several hours, a "nail-biting" experiment by IBM showed.

The technology giant sent 1,600 employees of an undisclosed healthcare company phishing emails - half generated by human social engineers and half crafted by AI.

The "humans emerged victorious, but by the narrowest of margins," IBM said in a report published published Tuesday.

Phishing is one of the most common ways to deliver malware, with 84% of organizations in Proofpoint's State of Phish report experiencing at least one successful phishing attack during the last year.

Several generative AI models, including ChatGPT, have a built-in protection meant to stymie malicious use - which researchers and hackers have easily (see: Yes, Virginia, ChatGPT Can Be Used to Write Phishing Emails).

It took the researchers just a handful prompts to break ChatGPT's block against writing phishing emails and trick the model into developing "highly convincing phishing emails in just five minutes," said Stephanie Carruthers, IBM's chief people hacker, who led the experiment.

"Most of my time was spent crafting the prompts and finding the right number and type to produce the most effective phishing email. After several hours of trial and error, I selected five prompts and fed those into the LLM to get it to create the phishing email. I didn't directly ask it to write a phishing email - instead I asked it to create an email based on the prompts," she said.

Her team usually takes about 16 hours to build a phishing email, which meant that using AI for the same purpose potentially saved users "nearly two days of work."

While it is possible to trick a commodity large language model to write a phishing email, making the task much easier and more efficient for attackers, it is only currently possible "if they put in the work upfront building the right prompts," Carruthers told Information Security Media Group.

The team generated the "highly cunning" AI phishing email, taking into account top areas of concern for employees in the target industry - healthcare in this instance. They instructed it to use social engineering techniques such as trust, authority and social proof, and employ marketing techniques including personalization, mobile optimization and a call to action. They also pointed to the person or company it should impersonate - the internal human resources manager.

To validate the experiment, IBM's social engineering team crafted its own phishing email "armed with creativity and a dash of psychology." They gathered open-source intelligence from social media platforms, the organization's official blog, Glassdoor and undisclosed sources. They sent this email t employees of the same healthcare company. The human element "added an air of authenticity that's often hard to replicate," Carruthers said.

The human-crafted phishing emails outperformed the ones generated by AI in terms of the number of people who clicked on a malicious link, albeit by a small margin at 14% and 11%, respectively. The former's edge primarily came from the humans' ability to understand emotions "in ways that AI can only dream of," and their ability to personalize content and keep it succinct.

Headline News...Cont'd

Carruthers said the AI-generated phish "lacked emotional intelligence and still felt robotic to me. That's why ultimately humans came out on top," she said.

While humans may have narrowly won this match, and cybersecurity researchers have not witnessed wide-scale use of generative AI by threat actors, Carruthers predicts that AI could outperform humans one day. How far away is that day? "If you would've asked me that question before this research, I would've said maybe a year or two. But after seeing the AI generated phishing emails, and the speed at which it was able to create them, I'd say maybe three-six months we'll see that gap tighten even further," she told ISMG.

The use of AI in phishing attacks means that companies must reevaluate their approach to cybersecurity. They don't have to fully revamp security awareness programs just because AI now helps attackers write more effective phishing emails, but they should start to incorporate the latest techniques, such as voice phishing, and prepare employees for more sophisticated phishing emails, she said.

Carruthers advised that organizations abandon the stereotype that most phishing emails are riddled with bad grammar and spelling errors, as AI-driven content removes these red flags. Longer emails, often a hallmark of AI-generated text, can be a warning sign, she said.

Upcoming Events

E-CRIME & CYBERSECURITY TRANSPORT ONLINE 2023
November 1, 2023
United Kingdom, London

PLANET CYBER SEC CONFERENCE
November 8, 2023
Long Beach, California U.S.A

BLACK HAT MIDDLE EAST AND AFRICA
November 14, 2023
Riyadh, Saudi Arabia