Department of Information Technology

CYBERSECURITY
AWARENESS
MONTH 2023

Date: 10/09/2023

Prepared by: Security Awareness	**Office of Security Management**	**Department of Information Technology**

Authentication and Passwords

Welcome to week two of National Cybersecurity Awareness Month. This week, we will focus on authentication and passwords. We have so much to remember every day. Add to that the dozens of passwords and PINs we must recall to log in to work and personal accounts, and it's easy to feel overwhelmed. And when we're overwhelmed, it's easy to let good security habits lapse. Passwords and PINs protect so much sensitive data. Using good password management practices is a great way to remain cyber-safe! Try these three best practices to keep your passwords and PINs safe.

#1 Create Strong, Unique Passwords and PINs

We know it's risky to reuse a password or PIN across accounts, but research shows that many of us do it anyway. We have password fatigue: we have too many accounts, and it's nearly impossible to remember complex passwords for each one.

- Fight the fatigue—According to SecurityBoulevard.com (link is external)
  - 65% of us reuse passwords
  - 91% of us know it's bad
  - 73% duplicate passwords across our personal and professional accounts
  - **422 million individual**'s accounts were compromised in 2022.
  - Compromised passwords are responsible for81% of hacking-related breaches
- Use strong passwords – passwords greater than 15 characters are generally very strong. But if you use upper case, lower case, numbers, and special characters, the chances of cracking a password become exponentially more difficult for the attacker.

Did you know that you can typically use spaces in your password? Choosing a short sentence or passphrase makes it easier to remember your password while creating longer, stronger passwords.

#2 Keep Your Credentials Secret

Protect your passwords and PINs like the valuable assets they are. Your login credentials are often the only things that protect your money and data from cybercriminals—keeping your credentials safe means not writing them down, not sharing them, and not letting others watch when you enter them.

- Don’t write down credentials. Avoid writing down PINs and passwords, even if you believe your hiding spot is sufficient.

- Don’t share your login. If you share your password or PIN with anyone, you can’t control what that person does with your credentials.

    1. What if your coworker writes your password down and leaves it in plain view?

    2. What if your coworker makes a mistake while logged in with your credentials?

    3. What if your credentials are passed on to someone outside your organization?

You could be blamed for someone else's actions using your credentials. Have you already shared your password? Change it now.

- Shield your credentials when you enter them. When entering a password or a PIN, shield your keyboard or keypad so that no one else can see what you’ve entered.

#3 Use Multifactor Authentication as Often as Possible

Multifactor authentication requires the use of two or more different factors to authenticate. The factors are defined as something you know (e.g., password, personal identification number [PIN]), something you have (e.g., smartcard, USB authentication token), or something you are (e.g., fingerprint, faceID). In addition to authenticating users at the system level (i.e., at logon), organizations may also employ authentication mechanisms at the application level, when necessary, to provide increased information security. It is always recommended to use multifactor authentication as often as possible, but it is important for protecting access to your most valuable systems, applications, and websites.

#4 Should You or Should You Not Use a Password Management Solution?

The answer to this question has become like answering the question - should you drive a car? Most security experts will tell you that storing passwords in a password management solution is a best practice. However, there remains little guidance on what solutions to use or practices to follow. And like the car analogy, it is because many options with different features affect the balance between security and convenience.

Password management solutions are a single point of failure. That is true. If the master password is forgotten, your account passwords held within it will need to be reset. If your master password is weak or someone watched you type it in and is compromised, the attacker will have all your account credentials.

So the first decision you must make is – Is a password management solution right for you? Is it worth the risk? Again, most security experts will say yes – IF you follow great password security guidance on choosing and protecting your master password.

One of the reasons many security experts find it difficult to recommend a particular solution for password management is because of the many options you can choose from:

1. Do you want your solution to store your password in the cloud or directly on your device?
2. Do you want your solution to create passwords for you?
3. Do you want your solution to enter your credentials for you automatically?
4. Will the solution be application-based, or will it be operating system or web browser-based?

These questions, and others, directly affect the balance between security and convenience, all of which are your risk decisions.

So, how do you choose what is best for you?

If you have decided that using a password manager is within your personal risk tolerance and you wish to leverage the convenience and security password managers provide, make your selection using the following considerations:

1. Define your requirements up front
    1. Do you want your password manager to only securely store your passwords?
    2. Do you want your solution to create passwords for you?
    3. Do you want your solution to remember the sites you go to and apps you use and automatically enter your credentials for you?
    4. Do you want a solution that works from only one device or all devices you use?
2. Choose a reputable solution
    1. Research the highest recommended tools from trusted security standards bodies such as the National Institute for Standards and Technology (NIST) or the International Standards Organization (ISO).
    2. Search for and read the customer feedback on the tools you are considering using.
    3. Give higher consideration to the tools with the greatest number of positive reviews.
    4. The table below shows the top 10 solutions by percentage of user base from 2021 and 2022.
3. Avoid “Free” password management solutions. There are two concepts to keep in mind around “free” software of any kind, especially when it comes to the security of your accounts and information:
    1. Nothing is ever free.
    2. You get what you pay for.

However, Free versions of reputable commercial password managers will often have the same level of protection for your passwords without additional features or other limitations.

1. Avoid using browser-based password managers
    1. Web browsers themselves have a history of weakness and vulnerability.
    2. Browser-based solutions limit your ability to use other browsers and apps.

In conclusion, using a password manager is a personal risk decision. Password managers are a single point of failure. But there is a significant precedent that shows password managers can be secure, convenient tools to help you protect your accounts and systems with long, strong, complex passwords that are unique for each account and do not require you to remember them. As we continue through October Cybersecurity

Awareness Month, take a minute to think about this topic and other ways to keep you and your families safe. As always, visit the doit.maryland.com’s cybersecurity website for more information. Stay cyber-safe.