MVNeighbors.org
@MarVistaNeighbors

Brain Drain

OR TRYING TO REMEMBER PASSWORDS

The average American has more than 200 accounts that require passwords. It is expected to double in the next five years.

Isn't this why we create an easy-to-remember password and use it on all accounts? Unfortunately, it also provides an ideal setting for hackers to gain access.

What's the solution? Password Manager software. Not only does the software remember all of your passwords, it creates them too, and works across all platforms and devices.

Due to the proprietary code of the software, passwords are not transferred easily to another program. So, take your time and research the various features and choose the one that suits you.

Once installed, you will be able to create strong and unique passwords for every account without having to remember them. This will free up some brain space for the fun memories, like those from attending the 2020 MVNA Annual Meeting.

The list is alphabetical; however, my personal favorite is Enpass.

- 1Password(1password.com)
- Bitwarden (bitwarden.com)
- Dashlane (dashlane.com)
- Enpass (enpass.io)
- KeePassXC (keepassxc.org)
- Keeper (keepersecurity.com)
- LastPass (lastpass.com)
- Myki (myki.com)

Mar Vista neighborhood association

Security Tip

This year make a special point of writing out the full year of 2020 when writing the date. If you write 1/23/20, it can be easily changed to a different date, such as 1/23/2018 or 1/23/2006.

SAFETY & SECURITY

Town Hall

Social Engineering

97% OF HACKERS DO NOT EXPLOIT TECHNICAL FLAWS, THEY EXPLOIT YOU!

We all know that the IRS doesn't call, and when we click that unknown email or URL, we authorize the installation of the hacker's software that will steal our information. Yet, the US represents more than 86% of all social engineering tactics called, "phishing." Social engineering is using psychological manipulation to trick users into providing sensitive information. It comes electronically, by phone, by mail, and in person. It is responsible for 91% of all data breaches, and is the single greatest threat.

What are some ways that you can protect yourself? First, recognize if you are in a favorite phishing pond. The following services make up over 95% of the industries targeted:

Email/Online Services (26.1%)
Financial (20.5%)
Payment Services (16.1%)
Cloud Storage/File Hosting (13.8%)
E-Commerce (7.6%)
Sofware-as-a-service (7.1%)
Social Networking (4.5%)

How many of these phishing ponds can you leave? Do you have multiple accounts in each category? Do you really need more than 1 payment service or cloud storage account? Must you have that software online/subscription, or can you be "old fashioned" and download it? Do you have to do online banking with every account, or just use online with those that are difficult to visit?

There is no way to stop attacks, but an attack does not mean a data breach. Use only companies that have withstood attacks and/or have good breach plans (for your security), and reduce the number of organizations that have your information. This is the best way to minimize your security exposure and keep your information safe. For more information, visit usa.gov/online-safety and consumer.ftc.gov/topics/online-security.

by Kathryn Wheeler

Spot a Fake

Request

A request of something FROM you: wire/send money; provide bank account numbers/info; personal info; in-person or remote access to your PC or mobile devices.

Private

You are asked to keep the matter private or a secret. All legitimate organizations encourage verification. Go online and research the phone number and/or address.

Urgent

By rushing you along, they hope to keep you off balance, limiting your natural ability to detect when something isn't quite right.

Authority

We've been raised to obey (and not question) authority. Attackers use this to their advantage and against us. They assume authority roles so we are more likely to obey without question.