### (Approx. 1390 words)

### Cyber Security

By David Kretchmar, Hardware Technician
Sun City Summerlin Computer Club
<https://www.scscc.club>

dkretch (at) gmail.com

Recently, SCSCC Vice President Tom Burt provided members with a link to an interesting article from *Malwarebytes* about cyber security: <https://www.malwarebytes.com/blog/news/2023/10/the-3-crucial-security-steps-people-should-do-but-dont>

*Malwarebytes* (2-week free or trial version) is an excellent product that other SCSCC technicians and I frequently use to search for malware and other potential PUPs (potentially unwanted programs) on computers. *Malwarebytes professional* is their paid-for real-time protection sold for $30 - $45 per computer per year.

**“Everyone’s afraid of the internet and no one’s sure what to do about it.”**

The essential point of the article was that many internet users employ "dismal cybersecurity practices" and are too lax in implementing and using security measures designed to keep them safe and secure. Some experts estimate that one-third of individuals experienced a security breach within the past year. This sounds reasonable based on my personal experience. Still, I also find it comforting that older adults (Baby Boomers) are estimated to be four times less likely to experience a security issue than younger users. I'm unsure if we are more careful than younger users or if we do less online.

While anything that makes people aware of the dangers that stalk all of us online is valuable, I disagree with two of the three primary points raised in the article. Malwarebytes provided the article, and since they sell subscriptions to their products to stay in business, it is arguably in their interest to frighten people, who then will be more likely to become customers.

In the following paragraphs, I will discuss the essential three points made in the article that I find misleading, outright untrue, and primarily true (multi-factor authorization).

## "Just 35 percent of people use antivirus software."

I call BS on this. It is rare for me to come across a computer that has no antivirus software running. Microsoft Windows Defender runs by default on Windows computers and does not have to be turned on by the user. This is by far the antivirus software utilized by most individuals, and it has the advantage of having no cost beyond what a user initially pays for a Windows PC.

In addition to being "free," the Microsoft Windows Defender program code is updated at least monthly. The monthly security update release is scheduled for the second Tuesday of each month. The Microsoft Windows Defender virus intelligence database is updated almost daily in case of newly discovered threats, also known as a 0-day or zero-day vulnerabilities. The term zero-day refers to the fact that the vendor has just learned of the flaw – which means they have zero days to address it.

It might be that only 35% of users subscribe to an antivirus software tool other than Microsoft Windows Defender. Certainly*, Malwarebytes* would like you to buy their product, but the article states an untruth when it says that only 35% of computers are protected.

I believe Microsoft Windows Defender provides excellent protection for most users. The modern version of this security package was implemented with Windows 10 in 2015 and is further improved with Windows 11. I have examined hundreds of computers since 2015 and have never had to remove a virus protected by Microsoft Windows Defender. Before 2015, our club's hardware technicians spent as much as half our time at our Tuesday Repair SIG removing viruses from systems, but this work is no longer necessary.

## "Just 15 percent of people use a password manager."

Again, I call BS on this. It is common for club members who come to the Tuesday Repair SIG when asked for their password to, for instance, their Google account to state, "I don't have a password; I just click on Gmail, and it appears." They are unknowingly and effortlessly using a password manager.

Without a password, you cannot use an application such as Gmail or any other mail program. Many users set up a password for Gmail or any other applications when they initiate use of that service or have this done for them by whomever is helping to set up their device.

Many users forget they have the required password because their browser's built-in password manager enters it automatically and seamlessly. Google, Edge, Firefox, and Safari all have integrated password managers with features like autofill and a password generator. They can also store credit cards and other personal information, which makes your online life more manageable. Smartphone operating systems on the Apple iPhone, Samsung Galaxy, etc. also store user credentials.

A password generator will create a unique password, such as "8X!4tZ7pas@vFyY" which is impossible to guess and memorize. A password manager best utilizes this bizarre string of characters. I have seen people write down and manually enter a generated password, but obviously, it is tedious and often takes multiple tries.

## Are passwords saved by browsers secure?

Google states, "Google Password Manager and the passwords it generates are considered safe compared to similar password managers. Google uses military-grade encryption to protect your usernames, passwords, and payment information."

Microsoft states, "Microsoft Edge stores passwords encrypted on disk. They're encrypted using AES, and the encryption key is saved in an operating system (OS) storage area."

Firefox states, "Firefox Desktop uses simple cryptography to obscure your passwords. Mozilla cannot see passwords, but Firefox Desktop decrypts the password locally so that it can enter them into form fields."

In other words, the "free" password managers built into browsers and operating systems use security schemes that are like paid password managers. Naturally, marketers of these paid-for third-party services, such as Nordpass, Norton, OneLogin, and LastPass, claim built-in password managers are vulnerable.

Unfortunately, third-party password managers have been hacked, severely compromising user information. OneLogin was hacked in 2017, and LastPass was hacked in 2022. In March 2023, LastPass stated that the breach resulted in unauthorized and unknown users gaining full access to customers' vault data, including personal information like usernames and passwords.

Yet third-party password managers urge users to buy their product rather than depend on the security built into browsers and operating systems. But any account or device can be hacked.

Unless you write down your passwords using a pencil and paper, you must trust someone and use a password manager. I would rather trust a massive entity like Google, Microsoft, or Apple over a relatively tiny software provider. Even more prominent entities, such as Norton, have been subject to internal dishonesty and theft of client data.

## Use multi-factor authentication (MFA)

This is NOT BS. Multi-factor authentication (MFA) requires users to provide at least two of three categories of authentication to access an account.

* **Knowledge:** a password or PIN code,
* **Possessions factor:** a secondary device (i.e., Smartphone) or account you have, in addition to a knowledge factor.
* **Biometrics:** any part of the human body that can be offered for verification, such as fingerprints or facial recognition.

I only have one account, Interactive Brokers, that *requires* MFA. When I want to access my account, a notification is sent to my iPhone, which opens the Interactive Brokers application on my phone and identifies me using facial recognition. Thus, all three factors of MFA are utilized, which is about as good a set of authentications as you will find today.

## Disadvantages of MFA

The second factor, the secondary device or account, is much stronger when a separate device is utilized. Many MFA schemes send a code to an email account, which is useless when that happens to be the account you are attempting to access. Using only an email account for secondary authentication rather than a discrete device, such as your Smartphone, provides weaker security.

MFA can lock you out of your account when your discreet device (phone) is unavailable, runs out of juice, or lacks an internet or cellular connection.

**Conclusions and Recommendations**

Microsoft Windows Defender runs by default on Windows computers and does not have to be turned on by the user. Microsoft Windows Defender provides excellent antivirus protection.

The password managers provided by browsers and operating systems are reasonably secure. I believe they are similar in security compared to password managers offered by third-party vendors, maybe better. These credentials operate seamlessly with the operating system or browser, making for a much smoother internet experience.

Multi-factor authentication is the way to go if you want absolute internet security. Using the three categories of authentication, knowledge, possession, and biometrics provides some of the best security available today.

