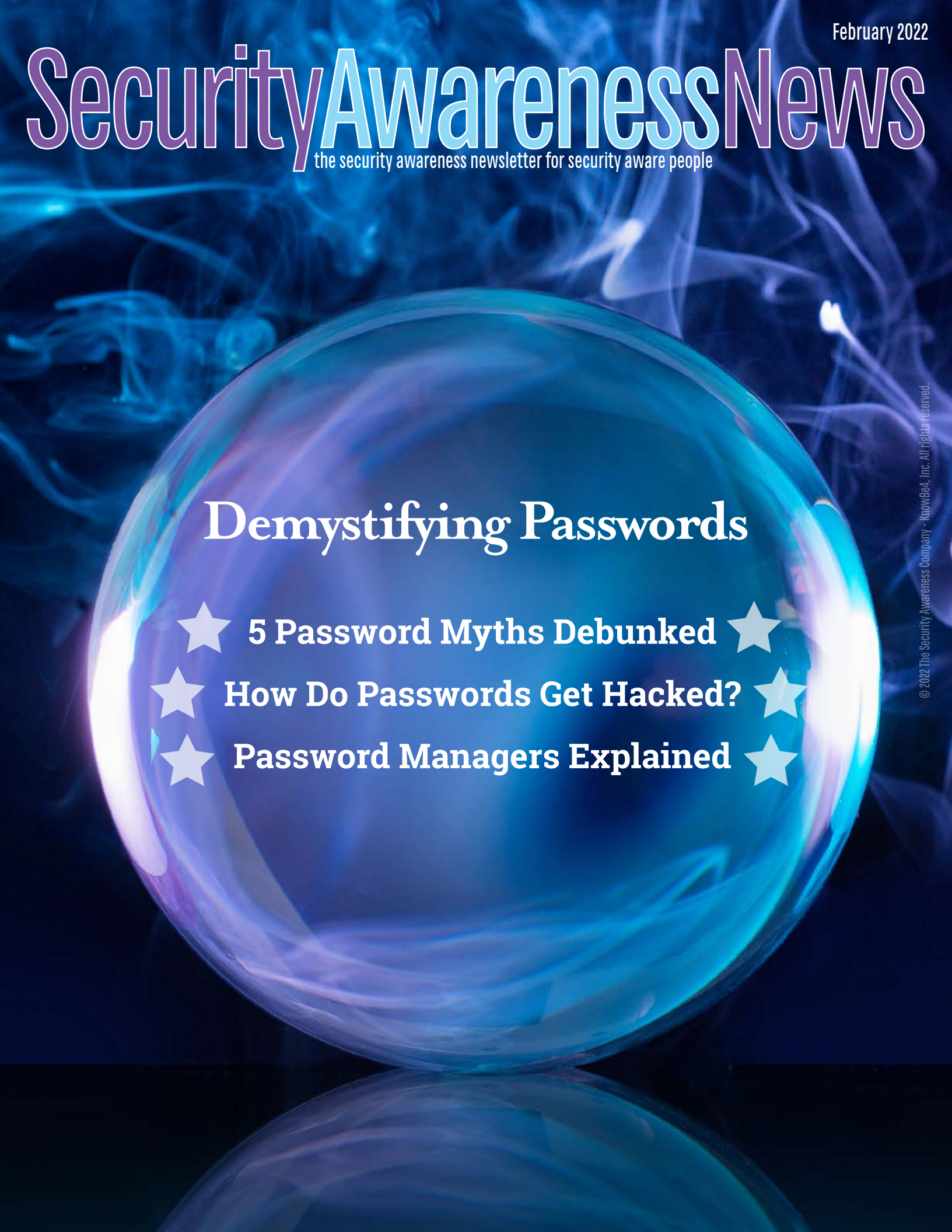
February 2022

SecurityAwarenessNews

the security awareness newsletter for security aware people



Demystifying Passwords

- 5 Password Myths Debunked
- How Do Passwords Get Hacked?
- Password Managers Explained

5 PASSWORD MYTHS DEBUNKED

The first use of computer passwords dates back to the early 1960s. Ever since then, they've been a source of debate regarding length, complexity, and effectiveness (passwords and the '60s). Let's run through common myths about the most primitive form of information security and try to unscramble a few password basics.

MYTH 1:

A strong password can be used across multiple accounts.

The problem with this thinking is that it doesn't account for data breaches that expose login credentials. When that happens, criminal hackers will use stolen usernames and passwords to see if they can access additional accounts via an automated process called credential stuffing. **Always use unique passwords for every account.**

MYTH 2:

Complexity trumps length.

You might think a random password like b3t5UD## is sufficient, but feel free to enter that password into any online password strength tester and learn how quickly it could be cracked. **Length equals strength! Ensure all passwords are at least 12 to 16 characters long.**

MYTH 3:

Regularly changing passwords improves security.

Ask five security professionals how often you should change your passwords and you might get five different answers. While changing passwords occasionally is never a bad idea, doing it regularly often leads to frustration and the use of inferior passwords. **Here at work, always follow password policies.**

MYTH 4:

All forms of multi-factor authentication (MFA) are equally secure.

MFA requires a second code before access to an account is granted—a vital part of security. Unfortunately, most people choose to have codes sent to them via text message or email—the least secure methods. **Wherever possible, consider alternatives to SMS or email, such as an authenticator app.**

MYTH 5:

Only highly sophisticated criminal hackers know how to crack passwords.

Sure, if a criminal wants to hack someone's password, they'll need a little know-how. But password cracking software is readily available, easy to use, and often free. Many versions can guess thousands of combinations in a matter of seconds. **Never use weak or commonly known passwords, such as password123.**

HOW DO PASSWORDS GET HACKED?

Social Engineering

The easiest way to steal someone's password is by simply convincing them to give it to you. That's how it's done by social engineers—the con artists who use manipulation to trick people into making poor decisions. They might, for example, call you and pretend to be someone from IT who needs your computer password to install a vital security update.

Prevention technique: Don't assume someone is who they claim to be. Never reveal your login credentials to anyone else.

Dictionary Attacks

As the name suggests, a dictionary attack involves using a list of predetermined words and phrases found in the dictionary and trying to log into someone's account via automated software. This attack is often successful because so many people tend to use easily guessed passwords that the software can crack in a short amount of time.

Prevention technique: Instead of a password, use a passphrase—a string of words forming a sentence that's easy for you to remember but difficult for others to guess.

Phishing

Clicking on a phishing link or opening a malicious attachment is a great way to have your password stolen. The link could take you to a fraudulent website that asks you to update your login credentials (which would send them straight to someone else). Opening a malicious attachment could install password-stealing malware on your computer.

Prevention technique: Think before you click! Stay alert for common phishing warning signs like a sense of urgency, bad grammar, and threatening language.

Password Spraying

Many systems implement lockout protocols that block access after a set number of incorrect login attempts. Password spraying circumvents those protocols. Instead of trying thousands of password combinations on a single account, the attacker "sprays" a single, well-known password (such as 123456) across multiple accounts. If unsuccessful, the attacker moves onto the next well-known password and repeats as necessary.

Prevention technique: Never use commonly known, weak passwords. Avoid passwords that use personal details such as the name of your pet.

Data Breaches

If you've ever heard about a data breach in the news that included the words "stored in plaintext," it means that the organization failed to securely store passwords of end users. That's how entire databases of usernames and passwords get exposed and made available to the public.

Prevention technique: Use unique passwords for every account. Enable multi-factor authentication wherever possible.

PASSWORD MANAGERS EXPLAINED

What is a password manager?

A password manager is software that can generate, store, and sync login credentials across multiple devices. There are many options available, each with slightly different features and price-points.

How does it work?

Password managers store your credentials behind one master password that unlocks the software. To log into an account, you simply enter your master password and the software does the rest. Whenever you set up a new online account, the manager can automatically generate a strong, unique password for that account, and save it on your behalf.

Most password managers will automatically fill online login forms with the click of a button. They can also store personal information (such as your name, address, phone number, email, etc.) and payment options (such as credit card data), and automatically fill that information as needed.

Should you use a password manager at work?

Simple answer: follow policy. Some organizations use password managers while others don't. Never install any unapproved software on work devices.

Should you use one in your personal life?

Generally speaking, yes. It's nearly impossible for most of us to remember the dozens and dozens of login credentials we need every day. Password managers solve this problem by requiring you to remember only a single, master password.

Are password managers secure?

There are two schools of thought to consider. On the downside, password managers could be viewed as a single point of failure. It stores every login credential you give it access to. If the developer gets hacked, it could mean that all of your passwords get exposed in a single breach. Big yikes. This has happened in the past, but it is extremely rare.

On the upside, password managers remove the hassle of creating and remembering strong passwords. This reduces the use of inferior or weak passwords and solves the issue of password storage. Most security professionals agree that the rewards outweigh the risks.