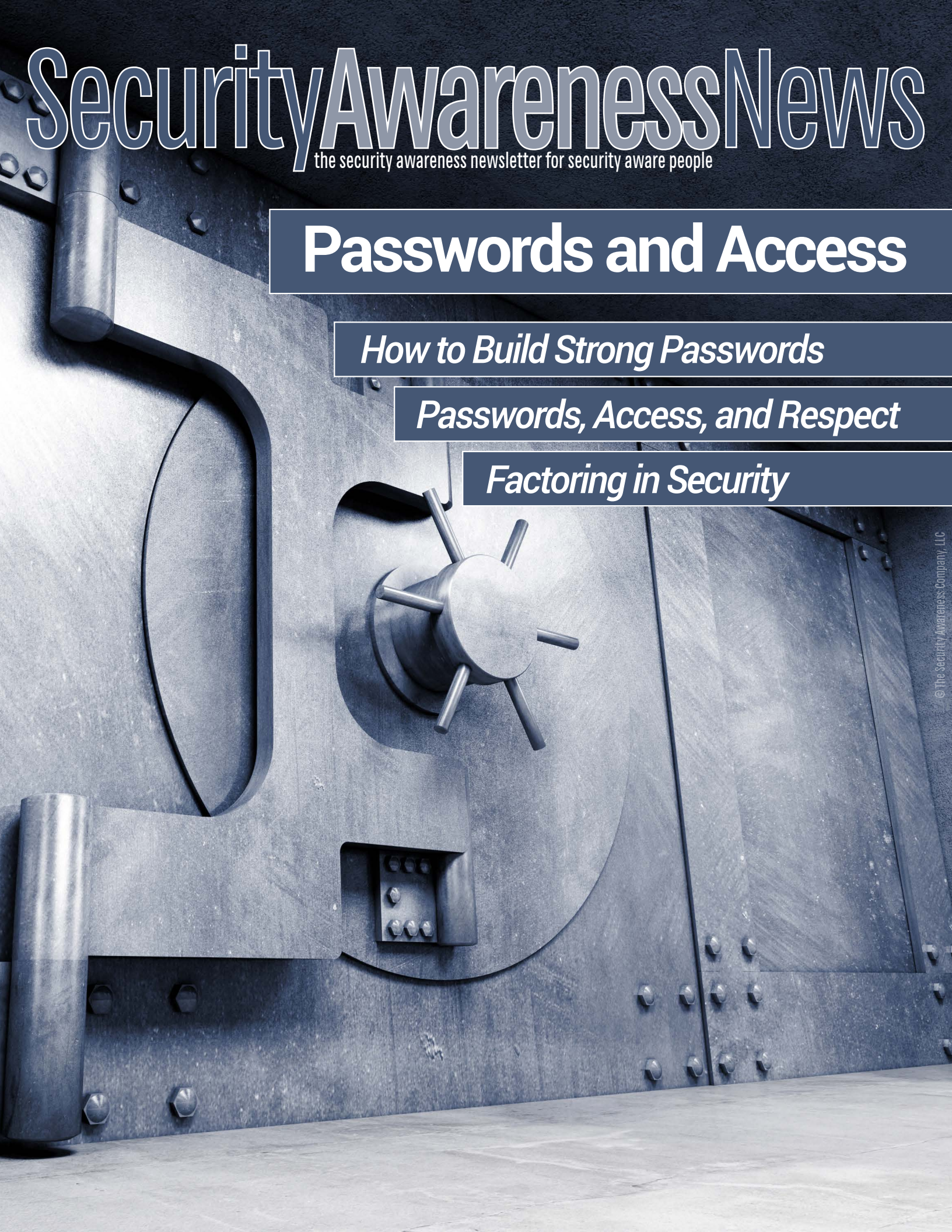
SecurityAwarenessNews

the security awareness newsletter for security aware people



Passwords and Access

How to Build Strong Passwords

Passwords, Access, and Respect

Factoring in Security

How to Build Strong Passwords

Thought exercise: which of these two passwords do you think is the strongest?

Asweaqf34$$a **VS** **unclebudsbestcatfish**

Given its randomness and complexity, the first option must be the strongest of the two, right? Actually, no. The second password, though it doesn't contain random characters or upper and lowercase letters, is the superior option. Don't believe it? Head over to a password strength checker such as "How Secure Is My Password" or Kaspersky's "Secure Password Check" to see for yourself.

The truth is, both passwords offer elite strength and would serve as great options for any type of account. But which one is the easiest to remember? Which one is easiest to type? The key to strong password creation is not complexity, but length and memorability.

Strong passwords in four easy steps:

STEP ONE

Pick a passphrase like in the example above (*unclebudsbestcatfish*). You're welcome to add numbers or special characters to strengthen it (and some systems will require a variety of characters), but it's generally best to take an ***"easy to remember, hard to guess"*** approach.

STEP TWO

Ensure it's at least 12 characters long. Of course, this may be limited by the requirements of by each login system but the longer, the better.

STEP THREE

Never use it twice. Using the same password twice is a great way for multiple accounts to be compromised, especially if that password is associated with a username that is your email.

STEP FOUR

Repeat for all accounts. Easy peasy. New passwords for each account that are easy to remember but hard to guess.

Here at work, always follow our predefined password policies.
If you have any questions, please ask!

Passwords, Access, and Respect

What's the fundamental purpose of passwords?

To prevent unauthorized access, of course.

And what's a fundamental element of security?

Respecting the access you've been granted.

Every member of our organization has been given some level of access, such as to our intranet and networks, as well as physical access to our building or secured areas. We require everyone to protect that access by following these rules:

- **Never share your login credentials with anyone for any reason.**
- **Never allow someone else to use your badge or key to enter secured areas.**
- **Always ensure secured doors remain closed and locked.**
- **Report all security incidents without hesitation.**
- **Always follow our organization's security policies.**

Should you save your passwords in a browser?

Absolutely not. Security researchers have proven that if a cybercriminal gains access to your computer, they can steal every password you store in your browser. You can read more about that here: Hackernoon - Why You Should Never Save Passwords on Chrome or Firefox.

Obviously, a key part of that is "don't get hacked." But why take any chances, especially for accounts that contain highly sensitive data, such as banking info and personally identifiable information (national ID numbers, home addresses, phone numbers, etc.)?

But how am I supposed to remember all these usernames and passwords?

In your personal life, get a password manager! Password managers create, store, and sync your login credentials across multiple devices. They can also auto-fill login forms on your behalf, removing the need to store your passwords in a browser. Here at work, check our policies before installing or using any third-party software.

Factoring in Security

So you've created strong, unique passwords for every account. You've followed our password policies here at work and have chosen a password manager to use in your personal life. Your accounts are safe now, right? Not quite. What happens when a major data breach occurs and your login credentials fall into the hands of cybercriminals? What's to stop them from logging in to your accounts? And how would you even know if they *did* access your account? That's why it's imperative to set up multi-factor authentication (MFA) wherever possible. With MFA enabled, the attackers remain locked out, and you receive an immediate notification that someone is attempting to access your account.

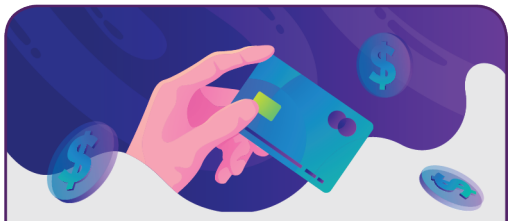
What is MFA?

MFA adds an additional security step—a second or third factor—as a part of the authentication process. It combines something you know, something you have, and/or something you are.

Something you know: Usernames, passwords, PINs, and security questions.

Something you have: Anything that you physically possess, such as a bank card, smartphone, USB drive, and security tokens.

Something you are: Biometrics such as fingerprints, face, eyes, and voice. This could also be your location or a physical gesture.



Everyday MFA

It is very likely that you have been using multi-factor authentication for years without even thinking about it, and it is probably in your wallet right now. Your bank card uses MFA. The first factor is the card itself—this is "something you have." The chip or stripe on the card contains encrypted information that identifies it as your card. The second factor is the PIN you use to authorize the transaction—this is "something you know." When combined, you are able to access your funds wherever cards are accepted.

Examples of MFA

SMS (Texting)
The use of this very common form of MFA will generate a one-time passcode via text message.

Email
Most accounts allow you to have the secondary code sent to an email address.

Push Notifications
Instead of receiving a text or email, users are prompted by a smartphone notification that asks if they're trying to sign into an account.

Authenticator Apps
Mobile apps that generate a one-time passcode that changes after a short period of time.

When setting up MFA, it's highly recommended to avoid SMS or email, since text messages can be intercepted, and emails can be hacked. Push notifications and authenticator apps offer stronger security because they require physical possession of a device.