September 2017

Security Awareness News

the security awareness newsletter for security aware people

The Front Door: *How Do I Get In?*

How to Build A Strong Password *in Five Easy Steps*

The Future of Identification and Authentication

PLUS: The 10 Most Common Passwords of «2016»

PROVEN PASSWORD POLICIES

If there's a single element of information security that we can point to as being the golden standard, it's passwords. To date, nothing carries more weight than the symbols, numbers, and letters we choose to guard our accounts and protect our data—both at work and at home.

This is why it's so important to carefully create those passwords, and to ensure that they are used once and only once, meaning every account, every login, deserves its own personal passcode!

At work, always follow policy regarding how passwords are generated and stored. And at home, consider developing a password policy for your entire household.

HOW TO BUILD A STRONG PASSWORD IN FIVE EASY STEPS:

STEP 1: Pick a phrase with at least three words you will remember.

We're going to need a bigger boat

STEP 2: Next, shorten it by using only the first letter of each word

wgtnabb

STEP 3: Then mix in upper and lower case

WgtnaBB

1702WgtnaBB

STEP 4: Now add numbers that mean something to you

#1702WgtnaBB!!!

STEP 5: Finally, add symbols

FIVE INDICATORS OF THE WORLD'S BEST PASSWORDS:

UNIQUENESS	Using the same password twice is a HUGE security risk. If it gets cracked, criminals will leverage that same code against multiple sites hoping to break through.
LENGTH	While there is some debate about how many characters should be required, there is no disagreement that longer is stronger. Length is better than randomness!
SNL	Symbols, numbers, and letters; every password should have a few of each.
CASES	Mixing up letters with upper and lower case is an easy way to strengthen your password.
PHRASES	Even better than standard passwords, passphrases (such as a quote from your favorite book or a beloved song lyric) are easy to remember but hard to guess!

Personal Security

ARE PASSWORD MANAGERS SAFE?

The short and easy is answer is, "Not 100%." There is no such thing as perfect security. But that doesn't mean password managers are unsafe, either. They store and sync your passwords through the cloud, which immediately presents a security risk. We've already seen a few instances of password managers getting hacked and users having their sensitive info out in the open.

But that's a rare situation. What you need to know is that ***they are much more secure than having a browser save your passwords, and certainly a much better option than using the same password over and over again.*** And, for that matter, most password managers have an option to store locally, eliminating the cloud and any chance that your information can be stolen in the event of a breach. So, in the end, password managers are one of the best tools for improving your personal security. Are you allowed to use a password manager at work or on a work-issued device? Please ask if you're not sure!

TO READ MORE ABOUT WHY YOU SHOULD CONSIDER USING A PERSONAL PASSWORD MANAGER, CHECK OUT THIS BLOG!
https://www.thesecurityawarenesscompany.com/2016/11/17/password-managers-yes-theyre-safe-yes-need-one/

Good security comes from timely response. Report security incidents immediately!

BAD PASSWORDS

THE 10 MOST COMMON PASSWORDS OF 2016

1. 123456
2. 123456789
3. qwerty
4. 12345678
5. 111111
6. 1234567890
7. 1234567
8. Password
9. 123123
10. 987654321

Do you see a problem here?

You should. In a study conducted by password management developer, Keeper Security, 17 percent of the 10 million passwords analyzed were "123456". You don't want to be anywhere near the 17 percent!

DEFAULT IS YOUR ENEMY

Perhaps you've heard of the Internet of Things, otherwise known as the IoT. Among its many capabilities, this network of connected smart devices allows us to control the temperatures and lights of our homes while on the road. But they've also allowed cybercriminals to carry out distributed denial-of-service (DDoS) attacks which shutdown servers and knock websites offline across the world. How? By taking advantage of default usernames and passwords. A lot of this issue could be solved if manufacturers put security at the forefront of new tech, but, in the end, ***it's on all of us to update default usernames and passwords ASAP*** whenever we hook up the latest and greatest gadgets!

FAST FACT:
7 of the top 15 most used passwords are made up of six or fewer characters, allowing brute-force attacks to unscramble them within seconds.

BRUTE FORCE ATTACK
A trial-and-error method to decode encrypted data using exhaustive effort (aka brute force) rather than intellectual strategies

WHY IS USING THE SAME PASSWORD FOR MULTIPLE ACCOUNTS DANGEROUS?

Because when a large company or database gets hacked, the criminals will use those stolen passwords and attempt to login to other accounts, such as banks and credit cards. By using unique passwords for each account, you insulate yourself from subsequent damages caused by breaches.

SECURITY TO THE POWER OF TWO

If you've ever set up an online financial account, then you've probably been introduced to two-factor authentication or 2FA. How does it work? It's a simple challenge and response that involves you first entering in your username and password. But instead of being logged in, you are prompted to enter an additional PIN number or code, most often sent to a smartphone via text, or to an alternative email address. This authentication process requires the user to have access to more than one account in order to log in. Always follow our policy before setting up 2FA at work. If you're not sure, ask!

TRUE OR FALSE?

1. *It is acceptable to tell your password to your boss or your spouse.*
2. *Substituting numbers for letters that look like them (e.g. replacing "o" with "0") is a good way of making your password stronger.*
3. *Identification, authentication and authorization are collectively referred to as biometrics.*
4. *Your ATM PIN was the first form of IoT authentication.*

ANSWERS: 1. FALSE. Never share your passwords. 2. TRUE. 3. FALSE. They are referred to as 'access controls'. 4. TRUE. The ubiquitous money dispensers went online in 1974.

SOURCE: (https://blog.keepersecurity.com/2017/01/13/most-common-passwords-of-2016-research-study/)

Good security comes from timely response. Report security incidents immediately!

THE FUTURE OF IDENTIFICATION AND AUTHENTICATION

IN THE BEGINNING...

Passwords have been around since ancient times, back when you needed to know the correct word to pass or enter an area, and have evolved over the course of history to meet specific demands. The military developed a challenge and response system that required not just a password, but also a counter-password. For example, the challenge would be Mango, and the response to Mango would be Peach. This form of authentication verified both sides.

The first computer password was born out of necessity in 1961 at MIT for use with their CTSS—one of the first time-sharing systems, which is a computing resource used by multiple individuals. Since there were multiple people who had private sets of files, it made sense that each person should be given their own login and password. The rest, as they say, is history.

PASSWORDS ARE DEAD... *LONG LIVE PASSWORDS!*

To this day, the debate over the future of security rages on with passwords right in the middle. Some argue that passcodes are no longer adequate enough to protect accounts and sensitive data, and that the future of identification requires more robust methods of protection, such as biometrics, which remove the burden of storing multiple passwords in databases that can be hacked.

But yet, passwords reign supreme as the first line of defense, just as they always have. Why? ***Because biometrics aren't necessarily more secure, since they're impossible to change*** (you can change your password but not your fingerprint). And just like standard passcodes, biometrics are also stored in databases, which can be hacked.

The future of identification and authentication remains cloudy. The only thing we can be certain of is that passwords are a long way from being replaced as the golden standard.

Biometrics Definition: measurable characteristics used to identify people, such as fingerprints and irises.

TYPES OF BIOMETRICS

Fingerprint Scanners
Your smartphone probably already has this, and it's used for more than just passwords. The sensor is also used by fitness apps to measure things like heart rate and stress.

Facial Recognition
Many smartphones and computers now come with face scanners via the use of cameras.

Iris Scanners
Similar to facial recognition, iris scanners register your eyes and unlock your device when you look directly at it.

Voice Recognition
A few years ago, a number of banks and other financial companies started using speech patterns and timbre in place of passwords.

Hand Geometry
You've probably seen this in movies where a character places her hand on a reader and it opens a secure door.

Good security comes from timely response. Report security incidents immediately!

Access Controls

The Principle of Least Privilege

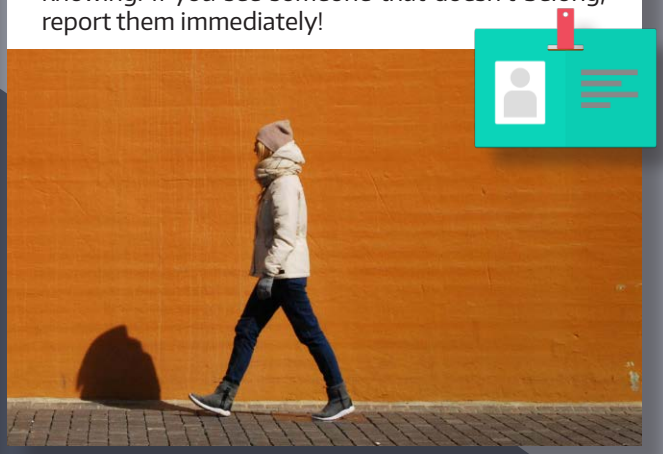
One of the most important things in keeping our data safe and secure is privileged access. Meaning, **WE HAVE ACCESS CONTROLS IN PLACE THAT DETERMINE WHO HAS ACCESS TO WHAT.** Why?

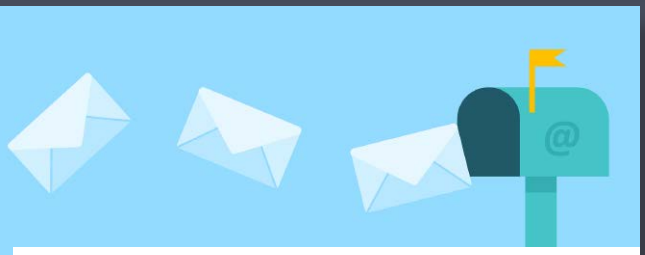
Let's use an example that applies to both work and home: the administrator account. The admin access allows you to make specific changes to how a computer operates. Would you want your child or roommate to have access to your admin account at home? Of course not. Even if you trust them with it, what benefit does it serve to give them access?

THE SAME IS TRUE HERE AT WORK. The principle of least privilege lets us grant you the minimum amount of access necessary for you to do your job. That way, if a breach were to happen or a computer were to get infected, it would be relatively isolated. This is why it is so important that you NEVER give out your credentials to anyone, and, if you feel you've been given more access than necessary, please say something!

Tailgating and Piggybacking

Access controls can also include badges or IDs that allow you to enter secure areas of buildings. But have you ever held the door open for someone after unlocking it with your credentials? If so, you've allowed them to piggyback, which is a security fail and violates policy! Similarly, **WE SHOULD ALWAYS BE ON THE LOOKOUT FOR TAILGATERS**—an unauthorized person slipping in behind an authorized individual without them knowing. If you see someone that doesn't belong, report them immediately!





Respecting Privileged Access

Consider the following scenario. You just received an email containing payroll information for the entire company. Essentially, you've just been given access to an extensive database. **WHAT DO YOU DO NEXT?**

A. Delete the email immediately.

B. Download the spreadsheet and scan it for viruses.

C. Inform a manager ASAP and tell the sender of the email they made a mistake.

D. Ignore the email and go about your day.

Correct answer: C. If you've ever been given access to something beyond the scope of your job function, report it immediately!

Access and Insider Threats

While our organization is always on the defense against cybercriminals, we also have to acknowledge possible internal threats to our sensitive information. These are known as insider threats and they include **everyone who has access to valuable assets.** In fact, the more access you have, the bigger the threat you are.

THERE ARE 3 TYPES OF INSIDER THREAT WE NEED TO BE AWARE OF:

The malicious insider:
One who purposefully undermines the operations of organization in some manner (such as intentionally stealing or leaking data).

The accidental insider:
One who unintentionally causes a breach or compromises our organization (such as accidentally sending sensitive information to the wrong party).

The negligent insider:
One who may not have malicious intentions, but knowingly breaks policy (such as using an unapproved, third-party file-transfer service).

This is why **YOU SHOULD ALWAYS FOLLOW COMPANY POLICY AND BE AWARE OF THE ACCESS YOU HAVE, SO AS NOT TO COMPROMISE IT IN ANY WAY.** If you're not sure what your role is in our efforts to protect information, please ask! There is no such thing as a stupid question.

Good security comes from timely response. Report security incidents immediately!