BIZ NET
BUSINESS - NETWORKS

THE Tech chronicle
October 2018

## EXPERT ADVICE

Check out these password tips from some security practitioners.

"If there's one thing I would advise everyone to do on their personal devices, it's to get a password manager. There are lots of free options out there, and many inexpensive paid options that will sync between all of your personal devices and machines. The manager will not only safely store and remember all of your passwords so you don't have to, but will also create strong passwords for you."

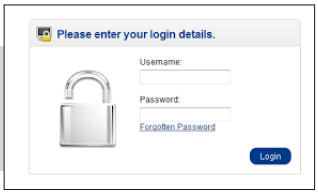
"I answer all of my security questions as if I were the lead character in my favorite book series. That way, no one can find my responses in my social media profiles."

"Longer is generally stronger than using random characters. It usually takes just a few extra characters to make up for a lack of different types of characters. So use full sentences whenever possible."

"If a site offers the use of multi-factor authentication, go for it! Additional layers of security are always smart."

# The Importance of Passwords

Have you ever thought about the underlying process of identification and authentication online (usernames and passwords)?




Who are you? (I'm this person) Prove it.
(Here's proof, usually a password.) Success!
Here's access to your important stuff!
Or, if you can't prove who you are? Fail! Try again…

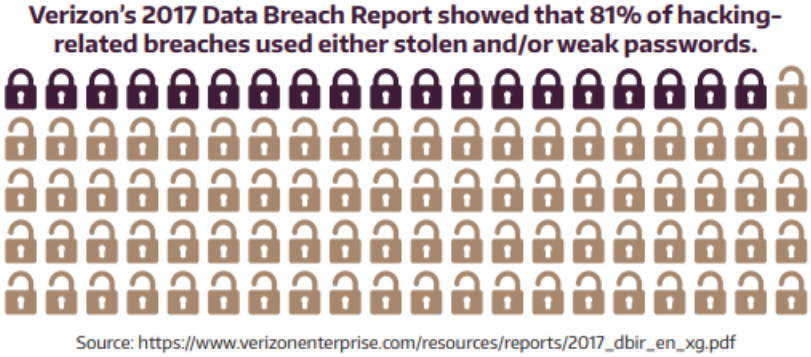
This simple question-and-answer routine has been around ever since human beings first had a reason to password-protect something. (Who goes there?) The amazing part is, that despite the massive technological changes that society has undergone over the years, authentication processes have barely changed. One would think that, given the stakes, proving identity would have evolved by now.

Instead, usernames and passwords still rule as gatekeepers with few alternatives on the horizon. Sure, they've seen a variety of complementary upgrades, like character requirements (symbols, numbers, letters), two-factor authentication, and biometrics (fingerprint scanners, facial recognition, etc.). But most accounts and devices still rely on the static Q&A without any additional rules.

Perhaps future advances in technology will provide an adaptable alternative to the current system. But until then, it's on all of us as individuals to take control of our password habits. That starts with following policy here at work and ends with developing a policy at home. Think about what's at stake when you create passwords for email accounts, bank accounts, online retailers, and so on. Inferior passwords make answering the "prove it" part of the equation too simple for criminals. Lock up your important stuff with strong, unique codes, and utilize twofactor authentication wherever possible!

**And remember, if you have any questions about your organization's password policies, please ask!**

Article provided by KnowBe4




Source: https://www.verizonenterprise.com/resources/reports/2017_dbir_en_xg.pdf

BIZ-NET
1325 Airmotive Way Suite 208
Reno, NV 89502

www.biz-net.com

This monthly publication provided courtesy of Marco Romero, President of Biz-Net, Reno NV

Our Mission: To provide the best possible service for our clients using the best tools available today. *As a business owner, I know you do not have time to waste on technical and operational issues. That's where we shine!*

# NEW PASSWORD GUIDELINES:

For the longest time, security experts have recommended long, complex, and sometimes random, passwords. Unfortunately, those guidelines create a dilemma for individuals and organizations alike. Of course, the more complexity you add to a password, the harder it is to crack. But a more complex password also means it's harder to remember.

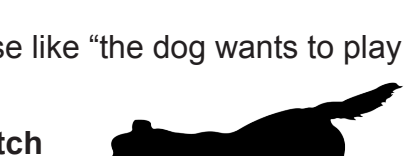
Complexity often fosters frustration, which in turn promotes laziness and tempts people to use the same password for multiple accounts. But there is hope! **Earlier this year, the National Institute of Standards and Technology (NIST) released a special publication of updated best practices for creating passwords.** Here are the highlights:

## Ditch the complexity.

Passwords that feature a bunch of random characters and capitalization no longer get the stamp of approval. Instead,passphrases that feature simplicity, now top the list of recommendations.

For example, the previous guidelines recommended developing a passphrase like "the dog wants to play fetch".

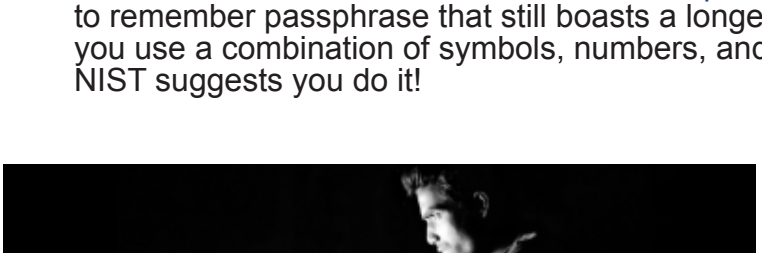
- But with a mixture of upper and lowercase letters: **TheDogwantstoPlayFetch**
- Next, add some numbers: **TheD0gwantst0PlayFetch**
- Then, some symbols: **TheD0gw@ntst0PlayFetch!**



And finally, your passphrase is complete. The problem? You've effectively complicated a supposedly uncomplicated process and created a hard-to-remember password.

Now let's apply the new guidelines to this same passphrase: thedogwantstoplayfetch

Done. No random characters. No random capitalization. No numbers or complicated features. Just an easy to remember passphrase that still boasts a longer-is-stronger attitude. There will still be systems that insist you use a combination of symbols, numbers, and letters. But when you have the option to use simplicity, NIST suggests you do it!



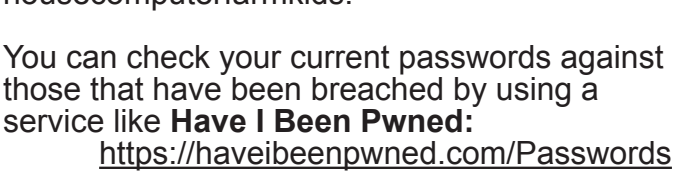
## End arbitrary password replacement.

Say goodbye to periodic or frequent password changes, a process that NIST suggests does more harm than good. Creating unique passwords for every account is already a difficult challenge. The new guidelines recommend only forcing changes if a security incident occurs which compromises existing accounts.

## Another secure idea.

Just like a dictionary list of previous breached passwords, over time we will see these phrases show up. We agree longer is better, and all lower case makes it easy, especially on phones. We recommend four or more 'random' words that are 4 characters each or longer. Such as: housecomputerfarmkids.

You can check your current passwords against those that have been breached by using a service like **Have I Been Pwned:** https://haveibeenpwned.com/Passwords




Biz-Net recommends having a few passwords, one for each category of account such as company, financial, social media, shopping, list services, etc. We also recommend monitoring the darkweb for breaches, and then change those accounts that contain any password that may have been breached.

Article provided by KnowBe4


| | |
|---|---|
| **Privileged Access** | The rights you've been granted to securely access data, networks, computers, and other integral elements of your organization. |
| **Access Rights** | The permissions you've been granted that allow you to read, write, and erase data. |

## Whats Your Role in This?

Respect the access you've been granted.

Use common sense, stay alert, and think before you click.

And remember that physical security is just as important as cybersecurity; don't let unauthorized persons access controlled areas of your organization, either by slipping in behind you or piggybacking off your credentials.

## Types of Privileged Accounts

**Local Admin Accounts -**
accounts used by IT and other management to maintain local computers, servers, and other types of workstations.

**Application Accounts -**
accounts used to access underlying company information that resides in databases and applications.

**Privileged User Accounts -**
accounts that provide admin privileges for systems and computers to specific individuals within an organization.

**Domain Admin Accounts -**
accounts that provide admin privileges across all computers, servers, and other types of workstations within the network or domain.

## Privileged Access at Home

Do you have parental controls set up in your household that prevent young children from watching certain content or accessing certain websites? That's a form of access control! As are user accounts on shared devices. And just like at work, it's important that the admin account be only available to the administrator and not to everyone in your household. For more parental control options, checkout out this article: https://www.thesecurityawarenesscompany.com/2017/04/20/best-parental-control-apps-keep-kids-safe-online/

## Anatomy of a Data Breach Using Stolen Credentials

Phish employee

v

Install malware on employee's machine

v

Steal admin credentials

v

Use admin account to access other services and machines

v

Exfiltrate sensitive data

Article provided by KnowBe4

BIZ NET BUSINESS - NETWORKS

# Protecting Your Business With Care For Your IT Services

## The Human Side of Security

Even with the most advanced technology in the world, our security posture is dependent upon a culture of security-aware individuals. This means that everyone here at work **(including you!)** must play their part in bolstering our organization's defenses. From the C-suite to the front desk, we all shoulder the responsibility of staying alert and using common sense in our day-to-day operations.

### 5 Things You Can Do Today to Strengthen Resilience to Cybercrime

(choose your role)

#### User

A person who helps keep our organization running on a daily basis and represents one of the most important elements of cybersecurity.

- **Always follow policy.**
- **Treat requests for sensitive info with skepticism.**
- **Know how to report security incidents.**
- **When in doubt, please ask.**
- **Develop a security policy for your personal life.**

#### IT/Tech/ Developer

A person in charge of developing, implementing, and managing our infrastructures and defensive strategies from a technical standpoint.

- **Keep systems up to date.**
- **Use caution when seeking help from online communities.**
- **Avoid allowing shared accounts or logins.**
- **Keep permissions restricted and document everything.**
- **Mitigate risky behavior.**

#### Executive/ Management

The top-level members of our organization who oversee our entire operation.

- **Lead by example.**
- **Participate in awareness training.**
- **Understand that you are a top target.**
- **Avoid oversharing on social media.**
- **Foster a culture of trust and communication within the organization.**

No matter your role, remember that security is a team sport! Every individual's effort, big or small, to protect our organization, contributes to our security-aware culture.

Article provided by KnowBe4