ACME FINANCIAL SERVICES

Powered by GLESEC

CYBERSECURITY NEWS CUSTOM REPORT

Generated on 02/21/2020 by Sergio Heker

Why Everything We Know About Passwords is Wrong

02/18/2020 15:37 Jennifer R. PoveyFeb 18 · 4 min read

Photo by Kaitlyn Baker on Unsplash

If you're anything like me, you hate passwords. My particular personal bugbear is the U.S. Copyright Office, which has complexity rules so arcane that I can't have my password manager automatically generate a password for it, and requires password changes every three months. Which I then have to write down somewhere because there's no chance of me memorizing it.

But that's what it takes to be secure, right?

Wrong, and cybersecurity experts who have been saying this for years are finally being listened to. NIST (National Institute of Standards and Technology) has issued a bunch of new guidelines. And those guidelines turn everything we thought we knew on its head.

Photo by Austin Distel on Unsplash

They're in this paper, but as I'm sure you don't want to read it I did so you don't have to:

1. Password length should be at least 8 characters if human generated, 6 if created by a machine, with a maximum length of at least 64 characters.
2. Special characters, including spaces, should be allowed but not required. In other words, they've finally admitted that those arcane complexity rules are a net security negative because none of us can remember our passwords. No other complexity rules should be required.
3. Password systems should prevent you from using passwords that were involved in known breaches, dictionary words, repetitive or sequential characters, the name of the service, your username, etc, and should tell you why you can't use that password.
4. Failed authentication attempt limits are a definite yes.
5. Passwords should not be changed periodically. This is a big one. While the guideline is to keep companies (I see you, U.S. Copyright Office) from forcing periodic password changes, what this basically says is that you don't need to change all of your passwords every few

months. In fact, it's bad because hackers target systems where passwords are changed frequently, and most people don't change them by enough anyway.
6. Passwords should be changed if there is any indication they have been compromised.
7. The system should let you paste in a password. This makes using password managers easier.
8. The system should allow you to opt in to seeing your password as it's typed. (This is for accessibility).
9. Multi-factor authentication is a good idea and should be used as much as possible.
10. Secret questions are a bad idea and need to go away. (Maybe they worked when the amount of time to find out somebody's mother's maiden name wasn't approx. five seconds).

There's also a bunch of new rules about encryption and the like.

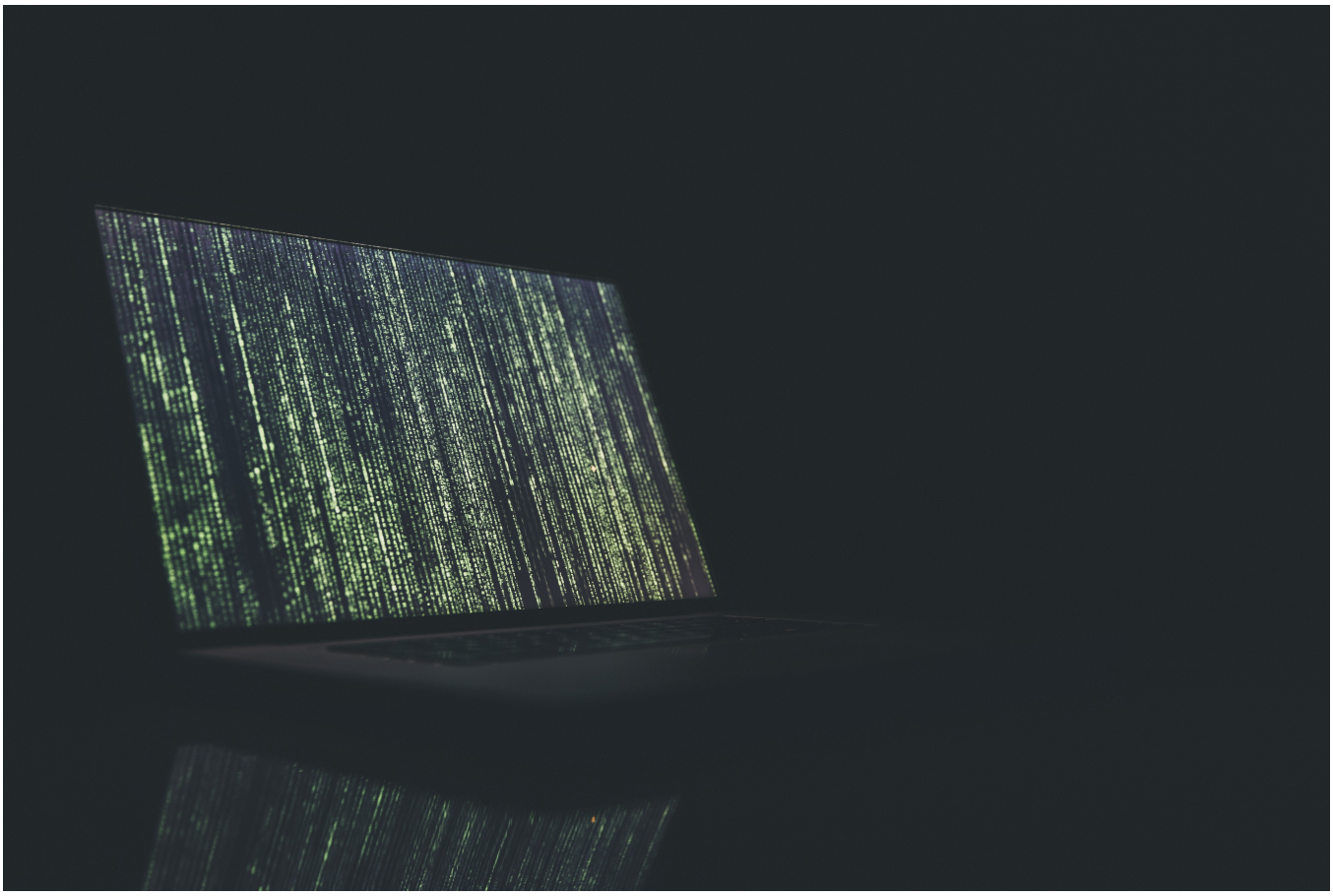

Photo by Markus Spiske on Unsplash

Assuming you aren't a sysadmin, in which case I'd hope you already know this stuff, then there's a few things you might want to change as a result of this:

1. Use pass phrases any time the system allows it. Pass phrases are much harder for a computer

to guess than passwords, and much easier for you to remember.
2. Don't change your password every three to six months. Change it only if you have reason to believe it's been compromised. Check haveibeenpwned.com periodically to see if any of your accounts were compromised.
3. Don't use the same password for multiple services. That's how a bunch of people got their Disney + accounts stolen. Don't blame Disney for that one.
4. Use a password manager. The ones built in to browsers are okay, but you should consider getting a separate password manager app.
5. Use multi-factor authentication on any service that allows it unless it becomes too much of a pain. Sometimes, unfortunately, it just makes the account unusable under certain circumstances.
6. If you're still being forced to use security questions, lie. Most especially never use your mother's maiden name (Whoever even thought that was a good idea).
7. If you must write down a password or the lies you answered security questions with, hide it and avoid noting which account it's for if possible. Don't store it on your computer.

So, basically? All of that "have at least one number and at least one special character and don't have three of the same character." (I see you again, U.S. Copyright Office) is all theater and no security, and it's finally becoming more obvious to more people that we need to all go change our passwords to something we can actually remember.

Unfortunately, it's very likely that most systems will still continue to require outdated and useless methods for a few years yet.

How is phishing still an effective way to breach companies?

02/18/2020 09:42 Digital LeadersFollowFeb 18 · 4 min read

Written by Victor G. Snyder, Consultant at BossMakers

When it comes to illegally infiltrating company data , there are various techniques that are employed by the 'bad guys' to garner the information they desire.

Many of us will think that brute force attacks and other forms of hacking are the most popular ways to get a foot in the door for the more nefarious members of the cyber world, but the truth is that phishing scams are still by far the easiest and most popular way for hackers to gain access to private and sensitive data.

The reasons for this fall into two major categories. Firstly, these attacks are easy to deploy, and secondly, we unfortunately seem to fall for them all too often.

Forms of phishing

So, how does phishing work ? Well, in a nutshell, phishing is the practice of fooling someone into relinquishing access to private information.

This can be something as simple as clicking a link that results in either being taken to a fake website or installing malicious code on a machine without the knowledge of the user.

It often takes the form of email correspondence that has a call to action, encouraging the user to click on a link in order to perhaps change an outdated password, pay an outstanding client, or log in to review some suspicious account activity.

When an email looks authentic, it is surprising how few users actually bother checking whether the URL on the link is correct or even if the email sender is official. To add further to these worries, it is worth knowing that the origin of an email can actually be spoofed anyway, so even the most diligent of users can still fall foul of this sort of scam.

To be fair to the majority of the workforce out there, these scams aren't always that easy to spot, and the ways in which phishing attacks are being deployed are getting ever more sophisticated.

A scam email from what looks like one of your company's usual suppliers asking to be paid can look every bit as legitimate as the real thing, especially to an untrained and busy employee who is trying to get through the workday as efficiently as possible.

You may think that these attacks are confined to the realms of the smaller companies out there, but anyone with an ear to the ground is well aware that plenty of huge data leaks at large corporations are still taking place across the globe.

While nobody is ever 100% safe from these sorts of scams, there are lessons that can be learned from each breach .

Educate your employees

Often, the best ways to stay safe from these attacks is to keep the advice you give employees as simple as possible. You cannot expect each and every staff member to know the intricacies of phishing attacks and how they work, but you can put into practice a set of rules that should lower the risks posed.

Making sure payments are made through official website portals, rather than clicking links within emails is easy to implement. It is also worthwhile making sure the whole company (or at least those with access to sensitive data and accounts) are comfortable speaking up when they feel something feels amiss.

One wrong move when you are faced with a phishing attack can lead to vast amounts of money going missing, or malicious software installed on your network that quickly turns into a ransomware situation.

With this type of attack seemingly going nowhere in the near future, more services are cropping up to deal with the threat, helping to train employees using simulated attacks as practice for real-world situations.

What are the next steps?

Ensuring that your team knows what to look for and how to deal with phishing attacks and drives down failure in detection rates for employees across the board. This, coupled with an automated phishing filter within an email client, is the best way to currently guard against this particular security risk.

Given the level of devastation that a breach can cause, more and more companies are turning to these measures to shield themselves. Any time humans deal with emails, there is always going to be some risk of human error.

If you can't totally eliminate a threat, the next best step is to minimize it. Those who don't manage to do so are all the more likely to find out the hard way just how devastating a phishing attack can be.

More thought leadership

Originally published at https://digileaders.com on February 18, 2020.