OCTOBER 15, 2021 // FRIDAY // ISSUE 2

SECURITY NEWS

BREACHED PASSWORDS: DON'T MAKE FOR THE BEST SECURITY

Fall Time is Officially Here.

Welcome Fall !!!

CHRIS MCDANIEL
SEPTEMBER 2021

The Yadkin County Information Technology Department would like to officially welcome the fall season. It's finally time again for cooler weather and warm blankets by the fireside. Since fall is rolling around we would just like to remind everyone to stay security smart. Let's not fall for phishing emails or fake scams as we start planning for the holiday season. It's that time of year when we all start planning our shopping list and there are cybercriminals out there that will continuously prey on the vulnerable.

This month's newsletter is going to focus on password protection. We are going to share information about breached passwords and how you can keep this from happening to you. We will discuss ways to make your information more secure and better protected from cybercriminals.

Breached Passwords

R. DALLON ADAMS, TECHREPUBLIC
SEPTEMBER 23, 2021

Specops recently released a roundup of the top 20 TV shows found on breached password lists. Shows like these offer plenty of entertainment, but they are not ideal for the inspiration of passwords. Sorry, "Cheers" fans.

Forgotten passwords can always be a pain and a general drag. As a result, people often resort to less than ideal cybersecurity strategies. On Monday, Specops Software, a password management and authentication company, released a new list of popular TV shows found on breached password list. While using your favorite program can make it easier to remember that Netflix password, following this logic could serve as a break in our cybersecurity armor.

"Attackers know making a strong, memorable password is hard and that people tend to choose easy things we know," said Darren James, product specialist at Specops Software, in a post about the findings. "This latest research shows us what we know to be true-that end users are making use of the things that come easy to them in their passwords, and that includes that old favorite show they've watched for years.

The inglorious list is based on more than 800 million breached passwords that Specops compared to TV Guide's Top 50 Shows and IMDB's Top 50 Most Watched programs. With more than 73,000 appearances on breached password lists. "The Flash" took the Number 1 spot in the Specops rankings.

While an almost new TV show claimed the top spot, associated shows were well-represented in the gathering. The 90s hit series "Friends" ranked second with more than 64,000 appearances on breached passwords lists, followed by "Taxi," the late 70s/early 80s classic starring Danny DeVito, Andy Kaufman, and Tony Danza, which appeared on the breached passwords lists nearly 59,000 times.

Next, "Arrow," "Elite" and Saturday Night Live" round out the top six, in order. Another blameworthy series and WB classic, "Buffy The Vampire Slayer," claimed the No. 7 spot, followed by "Lucifer" and "Vikings." Last but not least, the longest-running scripted show on TV, "The Simpsons," rounded out Specops' top 10, and the local watering hole-centric series "Cheers" made the list at No. 11.

The information for this article from TechRepublic may be found via the link provided here: Breached Passwords.

PASSWORDS AND TWO-FACTOR AUTHENTICATION

One Simple Step to Securing Your Accounts

Lysandra Capella, SANS, August 30, 2021

Example of How to Create a More Secure Password

Overview

Does it seem like cyber criminals have a magic wand for getting into your email or bank accounts and there's nothing you can do to stop them? Wouldn't it be great if there was one single step you could take that would help protect you from cyber criminals and let you securely make the most of technology? While no sole step will stop all cyber criminals, one of the most important steps you can take is to enable a feature called two-factor authentication (sometimes called 2FA, two-step verification, or multi-factor authentication) on your most important accounts.

The Problem with Passwords

When it comes to protecting your accounts, you are more than likely using some type of password. There are numerous ways to authenticate yourself into an account:

- Something you have
- Something you know
- Something you are
- Somewhere you are

When you employ more than one method of authentication, you are adding an additional layer of protection from cyber criminals – even if they crack one method, they'd still need to bypass the additional factor(s) to access your account. Passwords prove who you are based on something you know. The danger with passwords is that they are a single point of failure. If a cybercriminal can guess or compromise your password, they can gain access to your most important accounts. In addition, cyber criminals are developing faster and better techniques at guessing, compromising, or bypassing passwords. Fortunately, you can fight back with two-factor authentication.

Two-factor Authentication

Adding two-factor authentication is a more secure solution than relying only on passwords alone. It works by requiring not one but two different methods to authenticate yourself. This way if your password is compromised, your account is still protected. One example is your Bank card; when you withdraw money from an ATM or Cashpoints machine, you are actually using a form of two-factor authentication. To access your money, you will need two things:

- Your Bank card (something you have)
- Your PIN number (something you know)

If you lose your Bank card, anyone who finds your card cannot withdraw your money as they do not know your PIN. The same is true if they only have your PIN and not the card. An attacker must have both to compromise your Bank account. The concept is similar for two-factor authentication; you have two layers of security.

Using Two-factor Authentication Online

Two-factor authentication is something you set up individually for each of your accounts. It is very simple, you usually need to do nothing more than syncing your mobile phone or email with your account. This way when you need to log into your account, not only do you log in with your account username and password, but you also use a unique one-time code you get from your phone or email. The idea is the combination of both your password and unique code are required to log in. Usually, this unique code will be sent via a text message to your mobile phone or email. Your phone may also have a mobile app (like Google or Microsoft Authenticator app) that will generate the unique code for you. When possible, mobile apps are considered the most secure option for obtaining your unique code.

What makes this so simple is that you usually only have to do this once from any computer or device you are using to log in. Once the website of your account recognizes your device, moving forward you often only need your password to login. Any time you try (or someone else tries) to log in with your account but from a different computer of device, they will have to use two-factor authentication again. This means if a cybercriminal gains your password, they still can't access your account as they can't access the unique code.

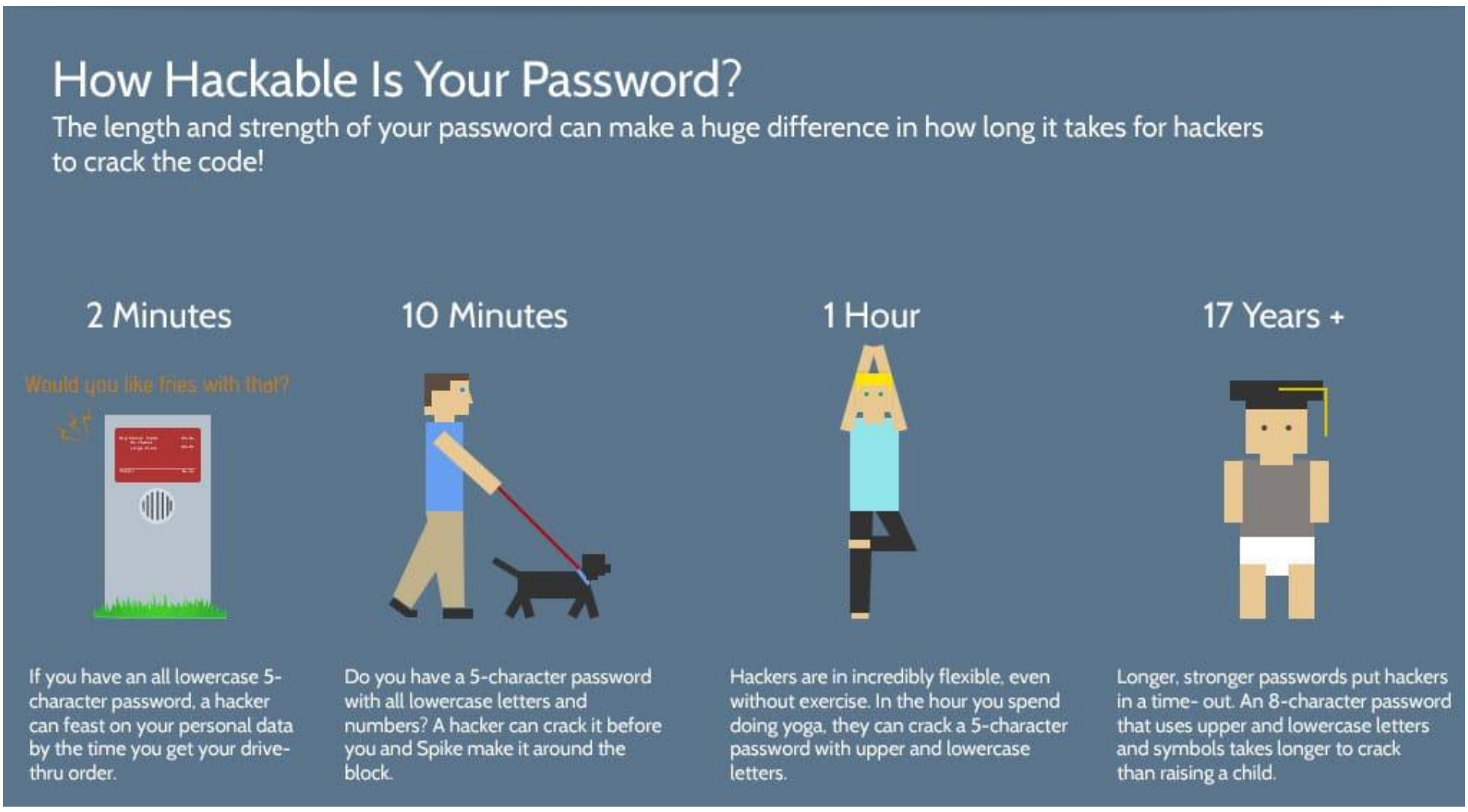
Remember, two-factor authentication is usually not enabled by default, so you will have to enable it yourself for each of your most important accounts, such as banking, investments, retirement, or personal email. While this may seem like more work at first, once it is set up it is very simple to use.

Other site that allow two-factor authentication are Google/Gmail, LastPass (Password Manager), Apple, Facebook, Twitter, Dropbox, PayPal, Microsoft Accounts, Yahoo! Mail, Amazon, and LinkedIn.

The information for this article from SANS may be found via the link provided here: SANS OUCH! Newsletter.

SECURITY NEWS

PASSWORD TIPS



TIPS FOR STRONG & SECURE PASSWORDS

October is National Cyber Security Awareness Month, so we've put together these tips for creating strong passwords to keep your accounts secure. From Facebook to your Bank account - security matters.

1 UNIQUE

Do not use the same password in more than one place. It is risky to use the same password for multiple accounts, because if a hacker gains access in one place, they'll have access everywhere else you have used the same password.

2 LONG

Longer passwords are more secure than short passwords. A good rule of thumb is to use at least 8 characters.

3 PHRASES

One simple way to meet the "long" requirement is to use more than one word as your password. Consider using a phrase like a lyric or a line from a poem.

4 VARIED CHARACTERS

It's always a good idea to include a combination of uppercase letters, lowercase letters, numbers, and special characters in your passwords. For example, if you were going to set your password as "happybirthday", instead set it as "H@ppyB1r+hD@y!".

5 AVOID PERSONAL INFO & COMMON WORDS

Avoid creating passwords with personal information that others may know or that would be easy for others to find out. For example: important dates (birthdays, anniversaries), nicknames, names of loved ones, your age, etc.

Also avoid using common phrases, like "happybirthday" or any variation of it, and patterns like "abc" or "123".

Now that you've created a strong password, keep it secure. Don't share your password with anyone, and if you need to write it down, don't leave it posted in view on your desk or computer.

Congratulations! Creating a strong password and keeping it secure is one of the most important steps you can take to protect your data.

INTELLITHOUGHT