frogworks

Managing Your Technology So Your Business Doesn't Croak.

May 2022

Issue 5 Volume 12

Ribb"IT" Review

INSIDE THIS ISSUE:

Why Data Breaches Happen

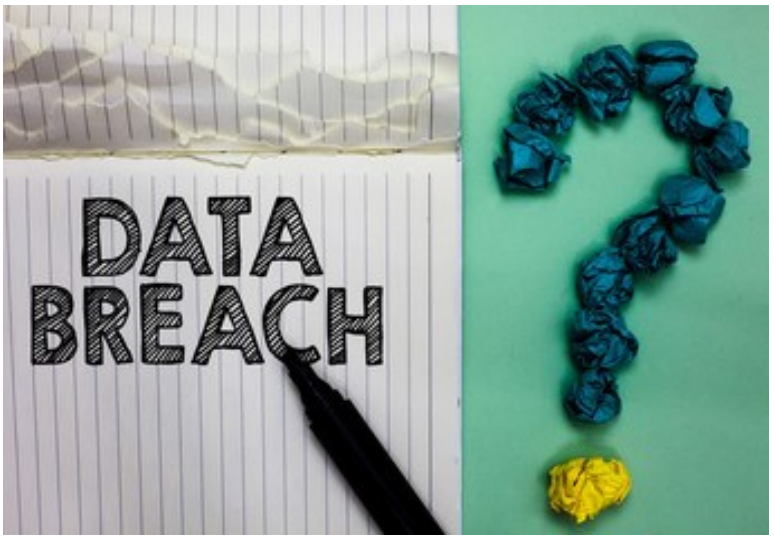
You may have survived the Data Breaches of 2021, but are you ready for 2022?

Are These Reliable Passwords?

If YES, Go to the next page!

If NO, Still go to the next page….

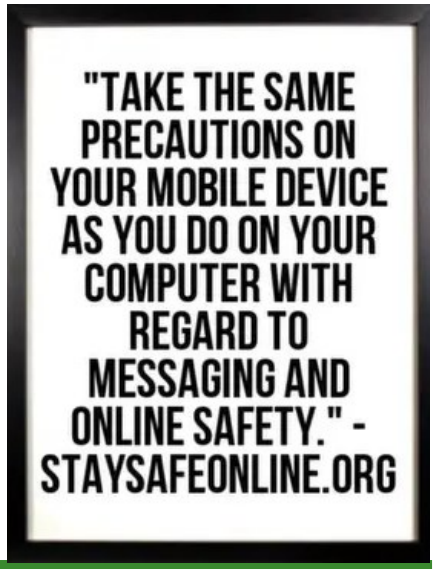
1. 123456
2. password
3. 12345678
4. qwerty
5. 123456789
6. 12345
7. 1234

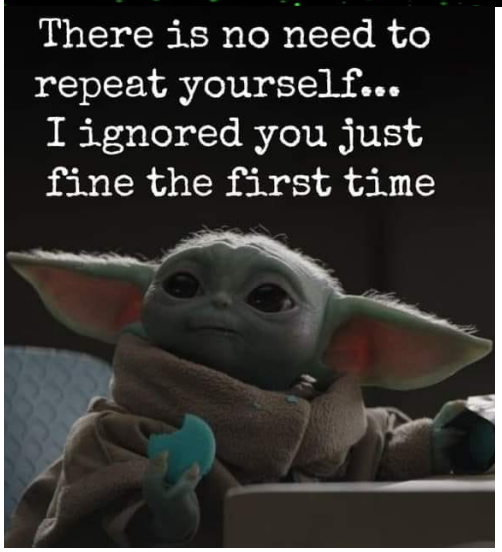


The world of Data Breaches and cybersecurity is a constantly changing one. With new threats emerging every month, it's important to stay on top of what the latest strategies for protecting your information are. This is so you can continue doing business without worry about becoming another victim in this ever-growing crisis.

The following articles will provide insight into how organizations have fallen victim. Frogworks has helped keep their clients safe from cyberattacks with new articles being published every month, stay up-to-date on the latest threats and tips to prevent being breached.

This monthly publication provided courtesy of:
Alex Bleam,
Owner of Frogworks





People Are Still Not Using Secure Passwords Despite Warnings

Answer: Those are the absolute worst passwords to use !!

It's 2022 and after years of warning people repeatedly about the dangers of using the same old passwords and using the same password across multiple websites, you would think this would get better. You would think we'd have that problem solved and there would be one less network security risk to worry about.

Unfortunately, if you think that you would be wrong.

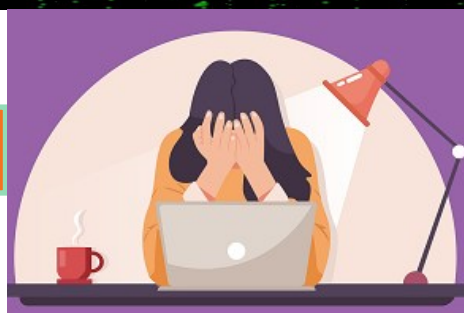
How does a password get hacked? Brute force attacks are when hackers take some of the most commonly used passwords and attempt to guess associated usernames. These automated processing systems allow vast quantities of input data, which makes them very effective at finding accounts with weak or newly created credentials.

PASSWORD RULES:

1. **Avoid using dictionary words.** These passwords are easiest for hackers to figure out.
2. **Try having 8 or more characters that are difficult to guess.** The best ones might seem difficult to memorize but that is what a password manager is for.
3. **Use special characters.** This technique is very effective and makes it harder for hackers to decrypt.
4. **Create different passwords for different accounts and applications.** This way if one password is breached, your other accounts won't be at risk.
5. **Don't use personal information.** Your birthday, name, social security number, and sensitive information you think is safe to use IS NOT.
6. **Don't use memorable keyboard paths.** Using memorable sequential letters and numbers, such as QWERTY are among the first to be guessed.

Use a password manager and a random password generator - A password manager keeps track of all of your passwords and does all the remembering for you, except for one thing — the master password. To get in there, we recommend using tips from before like using different characters or strings of numbers to make it more difficult; then use programs with generators such as Avast's Random Password Generator (see below) so you can come up with super complicated sentences!

Don't Fall For Fake Work Scams



Fake Work From Home Opportunities Are Phishing For Data

It's no secret that the pandemic changed the way much of the world works. Tens of millions of people are now working from home with millions more eyeing that as a very real possibility.

Unfortunately, the pandemic also changed what kinds of opportunities hackers and scammers are targeting. It shouldn't come as a great shock that they've begun targeting work from home opportunities.

Here's how a typical campaign plays out, according to researchers at Proofpoint:

On average, more than 4000 phishing emails a day are being sent to recipients worldwide. The bulk of recipients are in the United States, but people in Europe and Australia are being targeted too.

In more than 95 percent of cases, attackers are targeting email addresses that are linked to colleges and universities. So as a first necessary step, the attackers are either hacking into university databases to get the email addresses or they're leveraging someone else's prior breach and buying the data on the Dark Web.

In any case, the specific lure varies from one campaign to the next but it's always some variation of "we're hiring X number of remote workers to do this!" They then include a few details about the job with an attachment or an embedded link to follow for more information.

Naturally, if you open the file or follow the link you'll ultimately be presented with capture boxes designed to collect your login information or other personal details. If you give the hackers/scammers any information, you can bet that it will be used against you. According to FBI statistics, the average loss for a victim of employment fraud is about $3,000.

It may not be life ruining bad, but it still stings. In any case, these kinds of attacks are on the rise in our post-pandemic world. Be aware and make sure that your friends and family know too.

Warning Signs

- A job ad that claims no skills or experience is required.
- A company promises that a business opportunity is sure-fire and will pay off quickly and easily.
- You're required to pay upfront for training, certifications, directories or materials.
- It offers high pay for little or no work.
- The ad directs you to a non-business email address.

Scams you may see. And Should Avoid.

- Charity Scams
- Robocalls
- Fraudulent Links
- Email Impersonating
- False Advertising
- Covid-19 Scams

Samsung Breached; Hackers get Data Code

Source code is **the language or string of words, numbers, letters and symbols that a computer programmer uses**. An example of source code is someone using HTML code to create a screen.

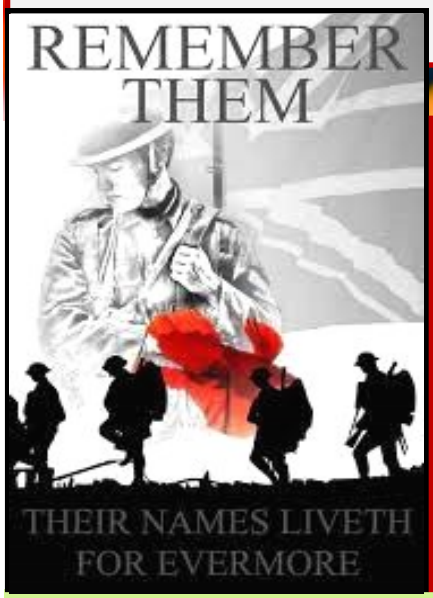
This March, **Samsung's** network was breached. Confidential customer information was stolen, hackers even got ahold of the source code for the software used in galaxy smart phones.

These hackers are called "Lapsus$". The worst part is, they do not know the full extent of the content of data. Lapsus$ has hacked various groups.

Disturbingly, this group has been exceedingly busy so far in 2022 and extremely successful. Just a week prior to the announcement regarding Samsung's data, the same group released a 20GB sample of documents stolen from Nvidia. The group claims that this sample is part of a collection of stolen documents more than 1TB in size.

Aside from the aforementioned source code at this point, we do not know exactly what sorts of data the group of hackers may have compromised when they successfully breached Samsung's network.

For that matter, we do not yet know the full extent of the contents of the 1TB cache documents stolen from Nvidia because as members of Lapsus$ explained, they are currently in negotiations for the sale of that data.



This is the world we live in. This is the shape of 2022 and years to come.

What You Need To Do

Be sure the software you use is updated with the latest security patches and constantly educate and reeducate your employees.

Failing that, take regular backups and have a rapid response team like Frogworks standing by that can spring into action if your defenses fail. That's by no means a perfect solution, but it will make

We Have an E-Newsletter!!!

Do we have your e-mail address??? If you would like to receive our newsletter though email please visit us at:

www.getfrogworks.com/newsletter

Channel Futures
Leading Channel Partners Forward

NEXTGEN 101

MSP TO WATCH • 2021 WINNER