Lightstone

ONLINE SAFETY TIPS

Unless you have been a **“hermit”** for the past 40 years, you should all agree that we all **live in an online world** now...

It is both the **“New Normal”** as well as a pretty scary place. Navigating this place in a **secure fashion** can be challenging and as usual, there is a lot of misinformation about security online.

The truth is that by taking a few simple steps you can make yourself much safer...

There are 3 basic super easy ways to do it, here’s the first:

1

Use a unique Password, but don’t worry too much about complexity...

Conventional wisdom says that, if you use a **long password** with **crazy letters**, **numbers**, and **symbols**, your account is safe.

The fact is, a password like: “annexrubykneadtone” **is just as secure as...** “J+e}F*b>J*S;36fSvbSLX)R}” as long as it’s **unique!**

When a hacker is trying to break into your account, the first thing they’ll probably do is **search through previous database dumps for your email address**. If you’re using the **same password** across multiple services, a **hacker who finds it can access many of your accounts**.

- There’s a **helpful website for checking** to see if your email address **has been included in a database dump**, but it doesn’t include every dump...
- If you are interested, **go try this with your personal and work email** addresses at: **https://haveibeenpwned.com/**

If you use unique passwords for each service, you know that **if one of them gets breached**, all of your **other accounts will be safe**.

This doesn’t mean that you should make your **password short and easily guessable**, obviously. And **don’t include any personal information** that could be easily researched.

BTW

...if one of your email addresses has been **‘pwned’**, just **change your password** and **use a unique one going forward**.

“When it comes to things like securing your hard drive or external drives with encryption, complexity actually becomes a little more important than it would be for an online service. Offline drives are susceptible to brute force attacks, where a hacker rapidly guesses millions of passwords.

There’s a surprisingly easy way to create strong passwords that you can memorize, refer to...

https://theintercept.com/2015/03/26/passphrases-can-memorize-attackers-cant-guess/

...BUT that will be able to stand up to a brute force attack.

You could also use this method for creating passwords for your online accounts, though it may be a little time consuming.

I don’t use this method, but I have a homegrown method that achieves a very similar result.

“I hope you will find this helpful.”

George, Group Technology Officer