8 Tips for Staying Safe Online! - Safer Internet Day 2020

Today is Safer Internet Day 2020, an annual campaign celebrated in approximately 150 countries around the world, in an effort to promote a safer and better internet. The internet's seemingly boundless creativity may be what keeps so many of us engaged, but for many the internet can cause some challanges. The conversation that should be an ever evolving one, and with today being Safer Internet Day 2020 it's a good opportunity for everyone to broach the topic of staying safe online. Here at Marshmallow, we have come up with a list of 8 simple things you can do to Stay Safe.

1 – Password Security

A strong password is key in keeping your account secure.

A good password should:

- A mix of Upper and Lower case letters and Numbers.
- Special characters or symbols (e.g. #)
- Be at least 10 characters long
- Never be reused

Strong passwords can be more difficult to remember, but you should still try to avoid reusing them.

The best password you can use is called a hash, this is basically a combination of entirely random letters, numbers and symbols. A hash could

be more than 64 characters in length, so a Password manager is critical in not getting locked out. (See Tip 2)

2 – Use a Password Manager

A much more ideal solution to dealing with the hundreds of passwords you could have is a password manager. Solutions such as LastPass make managing password security a breeze and as long as you have access to your password vault, you will never be locked out of an account again.

3 – Enable Two-Factor Authentication (2FA)

Two-factor authentication is an extra layer of protection you can enable on nearly all of your accounts. It works by requiring a confirmation, when your username and password is used to login to an account. From Google to Facebook to WordPress and even your Amazon account, 2FA protection is something you should enable to protect your accounts.

The best thing is, it's free and it's one of the most reliable means of locking your account down.

Most providers offer 2Fa in one of two ways, but both secure your accounts in the same way:

1 – Send a text message with a code to your mobile when you attempt to login

2 – Send a No

To turn 2FA on, just search online for whichever service it is and 'enable two factor' and you will be done in a matter of minutes. (e.g. Facebook enable two factor)

4 – Be cautious of links and file attachments

Links and 'dodgy' attachments are still to this day one of the leading causes of people falling victim to Phishing Attacks and other digital scams.

To avoid falling for digital scams and phishing attacks, do not carelessly open links and files send via email or social media.
Always be cautious of links that you have been sent, even from known senders. Examine the link before clicking it, the true location is normally shown when you hover over it. For example, say you receive an email ‘from’ Apple, but it links to somewhere entirely random, it is a good sign it’s not genuine!

5 – Keep your devices & software up-to date

We watch it time and time again, big companies who have been hacked, losing all that powerful customer data, all because they were using out of date software.
There is a simple solution really, keep your devices updated! Software updates contain vital security patches that fix new problems and bugs that have been found with your device and software. Left without these updates, your device becomes much more likely to fall victim to an attack as the bugs haven’t been removed.
As the years go on, Software and/or hardware will also need to be replaced. Technology unfortunately has a limited lifespan and this is the same for updates. When the time comes and updates are no longer being released, you are best to replace with new.
That means any old PC’s running Windows XP is absolutely out of the question, but you might be surprised to know that Windows 7 become end of life on the 14th of January 2020, this means that vital updates and security patches will be missing and you should look to upgrade as soon as you can.

6 – Have a backup of your data

I don’t know about you, but i have certainly lost a file or two in the past, back in the days before we had Cloud Storage so readily available.

One of the simplest ways to protect your data from loss or even ransomware is to keep a backup of your data. Whether it's your phone backing up to Google or iCloud or your PC with Onedrive or Dropbox a cloud storage solution is a great start.

For a business, you need more than this alone. What would happen if one of your Office 365 accounts get compromised and then deleted all your shared files, would you be prepared. In a world where staff have access to all data in a range of places, your data backup plan is critical for your business.

7 – Beware of Permissions granted to Apps

Too often, malware can hide in apps that look to be completely legitimate. Social Media apps that look like a bit of fun between friends can actually be malicious apps designed to harvest your sensitive data. For example, 'What's your Unicorn name', a new Facebook game that i just made up, might ask questions like:

1 – What is your mother's maiden name?

2 – What was your first pet name?

3 – What was your nickname at school?

Recognise these? That's because these are common security questions that you might have used to reset your passwords and lock you out! Sounds mean, but it's true and happens every single day!

Always be confident with the information you are providing to an app however fun it might sound! If it feels like a scam, it probably is!

8 – Use Weird (& Wonderful) Answers for Security Questions!

Where was you born? 'On the Moon' … Sounds weird right?! Well you're not wrong!

But you can guarantee one thing!... No matter how much searching someone does about you online, they are not going to get that answer! Maybe you did fall for one of those apps i just mentioned, not to worry, it’s not the answer! How do you answer those questions? Do you tell the truth, the whole truth, and nothing but the truth? Unfortunately, your truthfulness could be your biggest weakness, at least for account security!

So get creative with your answers and protect yourself from being locked out of your accounts today.