HomePage

Introduction

On this website is information about internet safety. This is meant to help and inform people about the potential dangers they may encounter as they explore the internet more and more. In order to learn about internet safety and how to strengthen it as well, continue reading below and check out the other web pages to learn more on a specific subject.

What is internet safety?

Internet safety is the act of making smart decisions online to ensure personal security and wellbeing. This takes many different forms from avoiding a hateful conversation to reporting dangerous activity you witnessed on social media. The root of all good decision making comes from personal judgment based on facts and logic.

Why does internet safety matter?

As we move further into the modern age, technology is becoming more important and included in daily life. The extent of how much one prioritizes internet safety directly affects not only them, but those around them as well. With wrong decision making, people can jeopardize the ones closest to them and leave them vulnerable to breaches in privacy. For example, if spyware were to be installed on a computer used by multiple people; not only would the person at fault have their information stolen, but all of the accounts tied to the computer would also be compromised.

Personal Security

Personal security is crucial to survive in the digital age, as there are an abundance of things people can do with other's personal information. Some are annoying while others are life threatening.

Personal Information

The golden rule of the internet is never share any personal information whatsoever. Doing so can actually put people in real danger as not only can their name and face be exposed, but their address too. This is a term known as doxxing, which is the method of publishing someone else's information online for the hope that another person will take advantage of it and harass the victim. This is most apparent in known figures such as influencers and they have been swatted by real police as a result of fake 911 calls.

This is alarming, but you can take steps to strengthen who can see your personal information. Firstly, never use your real name as a username on any application at all. This is a terrible decision as it makes finding out your real identity easy with just a quick glance. Secondly, don't willingly enter your information on websites without verifying its security, and be sure to delete the entered information as soon as possible if not needed. Lastly, don't add unnecessary data into websites such as location.

Digital Footprint

While users on the internet gain a sense of security behind their anonymity, their online presence is still being recorded. Once something is on the internet, it is very hard to make it disappear. There are plenty of cases in which people's online presence conflicts with their real world one. Employers as of late, have begun to investigate social media accounts of applicants before hiring candidates. More so, employees have actually been fired as a result of their postings on social media.

This really emphasizes the need for a clean digital footprint and there is a simple solution to achieving that goal. Creating a separate account is a great alternative to separate your business life from your personal life, rather than balancing both on one account. It is also the act of self-control; not posting hateful or illegal acts on the internet.

Harmful Software

Harmful software is the internet equivalent of a trojan horse. A usually promising or helpful application that has dangerous code to destroy or extract information from a pc. These are usually acquired by phishing links posing as something else. They are extremely damaging and can ruin an entire computer network. A malware is a software with the intent to siphon as much data as possible before being removed, while a virus seeks to destroy and ruin a computer system as much as possible.

Now you may be wondering how to fight back against these. The best way to stop harmful software is to prevent it from installing in the first place. Always avoid pop up ads and sponsored ads as they are the most likely to be phished. Before downloading, take a moment to analyze the source of the download and the download itself. If you do fall victim to a phishing scheme, be sure to have a reliable antivirus to detect it immediately so you can act without hesitation.

User Interaction

The anonymity the internet brings is a side effect that lets people act vastly differently than they do in the real world due to a lack of consequences and accountability. This leads to shady and outright criminal behavior that many will need to be able to identify and avoid.

Mindful Awareness

Cyberbullying

Identity Theft

First paragraph

There is no guarantee that you won’t be a victim of a data breach in a company, but you can reduce the accounts affected to only the account in question. This can be achieved by creating a new password for each individual account you make. The truth is, the reason people face breaches in so many accounts at once is because they use the exact same password every time, which leads to infiltrators reusing said password on different sites gaining access to those accounts as well. Keep track of accounts.

Harmful Content

Harmful content is a huge problem in today’s youth as it is practically spoonfed to them across social media in large quantities.

Gambling

Violence

Hate Speech