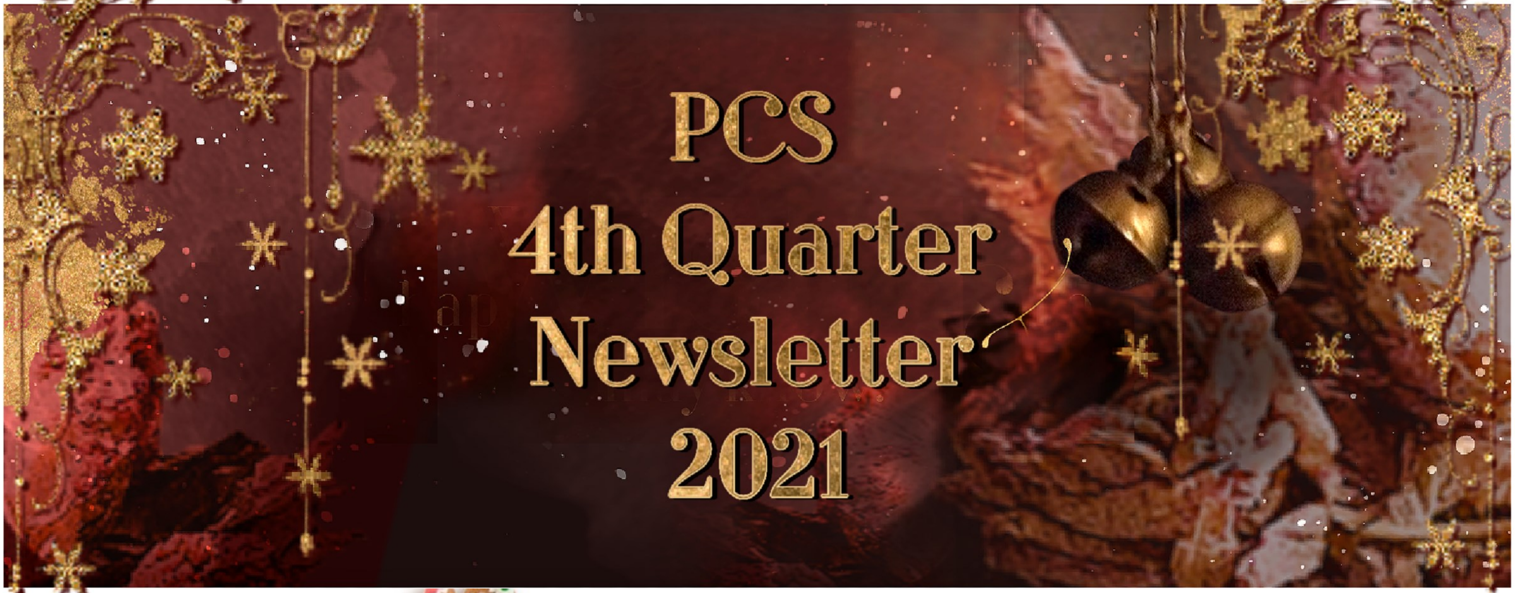


PCS 4th Quarter Newsletter 2021

THE DIFFERENCE BETWEEN Cookies & Cache

Anybody who uses the internet has come across the terms cache and cookies. These pieces of information are used to improve user experience and website performance. Both of them are stored temporarily on your computer or mobile device, but they serve different purposes.

In our cache vs. cookies guide, you'll learn what these two things mean, their main differences, and why you should clear them from your browser.

What are Cookies?

Cookies are messages stored in small text files. The sites you visit send them to your device so they can remember you and your performed actions. They typically contain things like the items in your shopping cart or the language you chose.

Cookies & Cache

CONTINUED

What is a Cache?

A cache stores some elements from the sites you visit, such as fonts, scripts, images, and videos. The purpose is to load pages quicker because rather than forcing your browser to download them again from scratch, you make use of the copies stored on your system.

Cache vs. Cookies – The Main Differences

Now that you know what cookies and cache are, let's take a look at the differences between them:

- Cookies remember users and their interactions on a site, whereas a cache speeds up the loading of web pages.
- Cookies store information like user preferences, while a cache includes the audio and visual content that makes up sites.
- Caches have to be manually removed every time. On the other hand, cookies are deleted automatically on some browsers.
- Caches store gigabytes worth of files as they hold static copies of content on web pages you visited. Cookies are relatively tiny and consume only a few KBs of space.
- Cache and cookies are both stored on your device, but they follow different routes. Cookies move from server to browser and vice versa. Caches, meanwhile, only travel from server to browser.

Cookies are often used by marketers to understand user behavior and serve relevant advertisements. However, a cache serves no such purpose and only makes your web browsing faster.

Why is it Important to Clear Your Cache and Cookies?

Cache takes up your storage and RAM, which slows down your device to a certain degree. Though sites will load faster on your mobile phone or laptop, other system functions might take a hit. To ensure the smooth operation of your device, it's recommended that you clear your cache regularly.

There are different types of cookies used by sites, but not all of them are good. Some of them (third-party cookies, for example) can be intrusive and collect information like your online habits, search history, and more. If you care about your privacy, your best bet is to delete your cookies regularly.

We use it, but we don’t think about it. Modern society is dependent on technology. Whether it’s your TV, the Internet, a laptop, or a phone, there’s no denying how much life has changed over the last two decades. This online access means that individuals and businesses need to be diligent about their Cybersecurity and Internet Safety.

We hear the terms *cybersecurity* and *Internet safety*, but are cybersecurity and Internet safety the same? The short answer is no. However, cybersecurity and Internet safety can incorporate many similar elements, and both involve online safety solutions. Yet, there are differences. Essentially, internet safety is about individual people and their safety, while cybersecurity is more about securing devices or information held on systems.

Internet safety

When we talk about Internet safety, we refer specifically to an Internet user’s awareness of their online safety. This awareness reflects their knowledge of the security risks to their private information. Many users are unknowingly open to threats to online safety. Their data and identities are juicy targets hackers are after.

With the rapid growth of the Internet, many services became accessible to users from all over the globe. Unfortunately, as digital communication increased, so did the incidence of malicious use for personal gain. This risk is a huge concern for children and the elderly, but anyone can become compromised. Common safety threats include internet scams, malware, phishing, cyberbullying, cyberstalking, sextortion, and online predators.

The awareness of internet safety is an important step for individuals in their private lives. This also applies to businesses and their employees. The risks they face are not only personal but also impact their organizations.

Cybersecurity

When we talk of cybersecurity, we refer to how organizations and individuals reduce the risk of cyberattacks.

The core function of cybersecurity is to protect the device rather than the individual. This protection also incorporates the services accessed at work and online from damage or theft. Finally, cybersecurity is about preventing any unauthorized access to personal information stored online and on devices.

Three key differences between internet safety and cybersecurity

1. Internet safety is about the protection of people, while cybersecurity is the protection of information.

2. Poor internet safety means that individuals are vulnerable on a personal level. Poor cybersecurity means that a system is vulnerable to hackers.

3. Internet safety relies on strong passwords, mindful downloading, and careful posting on social media. Likewise, cybersecurity relies on features like firewalls, up-to-date software, and multi-factor authentication.

Protect your business with an MSP

While both internet safety and cyber security are important, it is cybersecurity that businesses need to focus upon. One wrong move and the whole business could be devastated. However, business owners can be proactive in protecting their organization and their assets by hiring a Managed Service Provider to assist with their cybersecurity.

When a security breach can ruin your customers' trust and your reputation, businesses must consider cybersecurity seriously. Bringing aboard a Managed Service Provider is a proactive way for business owners to ensure they have the appropriate protection for their organization. Every MSP must stay up-to-date with the latest cybersecurity threats.

And for anyone who is ever online (most people!), it's essential to know all about Internet safety too. If you have any questions, feel free to contact us.

In conjunction with phishing, cybercriminals are also really good at psychology. In the Psych world, the psychological manipulation of people to perform desired actions is called “Social Engineering.” Cybercriminals, commonly put this social engineering concept into action with their phishing attacks against us.

Phishing techniques

Smishing - Fraudulent text messages are sent to trick you into revealing personal information or downloading malware.

Vishing - Voice phishing or phone fraud meant to entice you to divulge sensitive data.

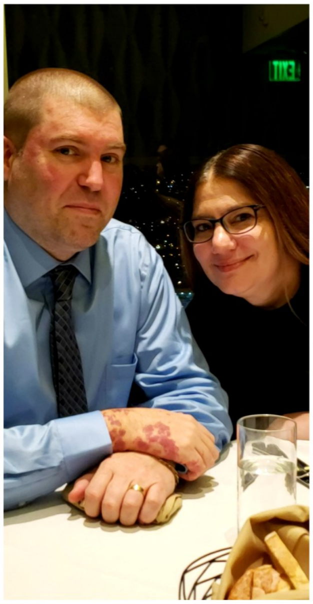
Email Phishing - Deceptive emails are meant to steal personal information or get you to click links to install malware.

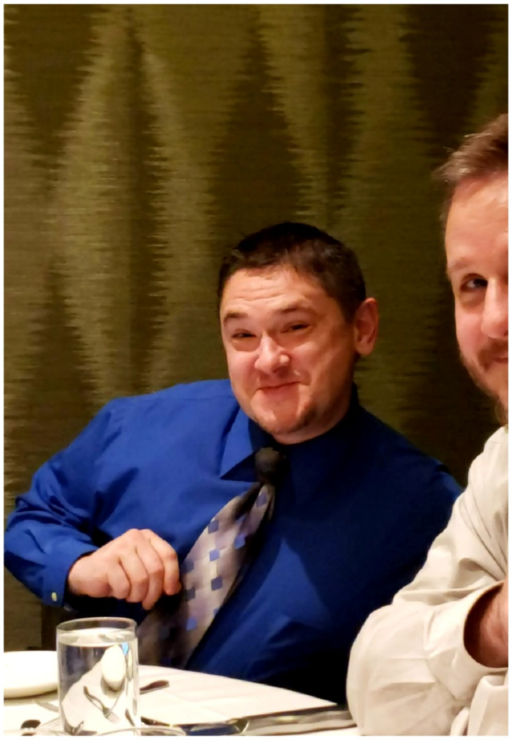
The reason these tactics work is because they exploit human trust. Trust, context, and emotion all play a role in decision-making and can easily be manipulated.

Using these methods, attackers will draft personalized messages that pose as legitimate organizations or individuals, regarding situations you’re likely to find yourself in, and create a sense of urgency around their desired action. Hook, line, and sinker.

There’s a lot of different ways cybercriminals can phish for your information and ruin your life or career. But find comfort in the fact that you can take control of your cyber-space. By taking your time and researching content that is intriguing to you before diving in (whether it be a hot new deal or a money-making opportunity), you’re creating boundaries that will protect you and your information from the unknown.

PCS CHRISTMAS PARTY PICTURES 2021





OLSKY
amazon
amazon

PCS
Season's Greetings
Season's Greetings

Happy Holidays and warm wishes for the New Year!

From all of us at PCS