PCS
Pittsburgh Computer Solutions

Newsletter

4th Quarter 2022

online shopping tips

Visual Spoofs

While online shopping is in full swing with great deals and flash sales flooding your inbox, it's easy to get wrapped up in the excitement. Before making that next purchase through a social media ad or unsolicited email, it's important to understand domain and website visual spoofing.

Visual spoofing is an action performed by a cybercriminal to disguise a website, or email for malicious purposes. With their disguise, there is a higher likelihood that their target will fall for the scam. There's many different types of visual spoofing techniques that cybercriminals use in their scams.

One type of visual spoofing involves Punycode attacks. These attacks use Unicode and swap out original characters for almost identical characters from different languages. Unicode does not unify these identical characters under the same code but instead treats them as separate letters or code numbers. This allows cybercriminals to imitate well-known websites or companies.

Another type of visual spoofing is domain spoofing. This occurs when a fake URL looks like a legitimate link but it's malicious. When examined closer, the fake domain often has additional letters or characters that the real site would not have.

These incidents are also called homograph attacks due to the use of similar characters that are not actually the same. Homograph attacks don't always use characters from different languages. The switching of the letter "O" for the number "0" is a common example.

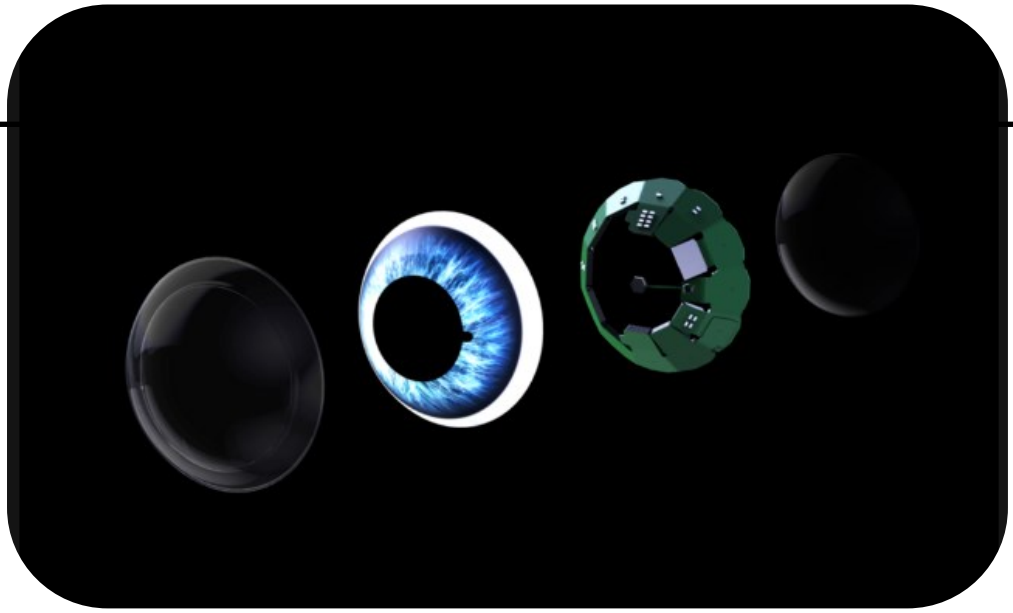
Once the cybercriminal gets a user in with a fake domain, they'll not stop there. Website visual spoofing refers to fake websites that cybercriminals create to mimic popular websites. They will copy the design, logos, and content of a website to make their knock-off look legitimate.

So, with all these advanced spoofing techniques, how can we all stay safe?

First, don't click on unfamiliar links. Always hover over a link before clicking it so you know where it is going to take you. There are times when the visual spoofing is so similar it's almost indistinguishable. Because of this, it's always better to access well-known websites directly by typing them in or searching them in a search engine instead of following a link. You can also use fake website checkers to help you decide if a website is safe.

Second, closely examine websites and domain names for any out of place characters or letters. Examine the website for fake logos, poor website design, and misspelled words. Look for accent marks over letters that would normally not be there.

Third, keep your browser up to date. Security patches and updates can help keep your browsing safe. By following these diligent steps, you will be able to have a great and safe online shopping experience.



Cool Tech

How Smart Contact Lenses Could Make Grocery Shopping Way Less Forgetful

People probably wouldn't forget something at the store if they taped a grocery list to their eyeballs. Definitely not recommending to try that. But a new prototype from smart contact lens maker Mojo would do something pretty similar.

Mojo announced a potential feature that would integrate Alexa Shopping Lists as an application on Mojo Lens, calling it the "first major third-party consumer application on a smart contact lens."

A user would be able to access the Alexa Shopping List in their frame of view, ask Alexa to add or remove items, and check off groceries as they're grabbed, all just by using their eyes.

If someone at home just finished the last of the milk, they could also remotely add an item, and it would appear in Mojo Lens as you shook your head.

Amazon believes experiences can be made better with technology that is always there when you need it, yet you never have to think about it. Alexa Shopping List. Mojo Vision's Invisible Computing for Mojo Lens, paired with the demonstration of Alexa Shopping List as a use case, is showing the art of what's possible for hands-free, discreet smart shopping experiences."

To be clear, this is just an early test and won't be available next week or anything. The Mojo smart contact lenses are still in early development as well. They'll have to figure that part out first, but demonstrations have shown they hope to achieve an eye-controlled user interface that augments activities, like seeing the trails while in nature or talking points for a presentation.

The idea seems to make it appear like you know what you're doing without people noticing that you're looking things up.

In any case, you probably won't need a grocery list to remember to buy eye drops while wearing a smart contact lens. This might be one of the best new items in the near future for technology.

You're likely aware we're facing a time of increased instability due to ongoing global events. These are being worsened by the continued efforts of cybercriminals to leverage this instability through a widening range of attacks focused not only upon critical infrastructure (e.g., power, gas, utility, and supply chains), but on business and individuals as well. We can't stress enough how important your actions to be a "human firewall" are to protect yourself, your company and ultimately, help thwart the efforts of bad actors around the globe at this time.

Here are some steps you can take to secure your business and personal data:

- Be on the lookout for an increase in phishing emails and social engineering tactics.
- Watch for banking, email, social media and other entertainment account compromises.
- Stay vigilant when utilizing links while browsing the Internet and within social media platforms such as Facebook, LinkedIn, and Twitter. This is especially so when you receive unexpected urgent messages.
- Ensure that Multi-Factor Authentication or MFA is enabled *wherever* possible.
- Be on the lookout for anything unusual. If something seems amiss, utilize the security policies, processes, and protocols within your organization before opening attachments or clicking links.
- If you click a link that takes you to a site, or otherwise, that you didn't expect...*notify* someone within your organization quickly and demand immediate activity to investigate, Don't assume that things will just be taken care of.

If you'd like additional information on cybersecurity and current threats call the experts at PCS and we'd be happy to help.

PCS

CHRISTMAS

PARTY

PICTURES 2022

Be merry

happy holidays

Winners of the Prize Wheel!

Thank you Dave & Lori!

SEASON'S Greetings