The Importance Of Keeping Up With The Cybersecurity Trends

“Convenience is the enemy of security. And the enemy of my enemy is my friend.” – Cybercriminals everywhere.

As internet users, we want processes to be streamlined: one-tap payouts, face scans to confirm installs, auto-logins with Google, and the browser remembering hundreds of passwords. But all of that saved time comes at a cost.

Photo by Florian Krumm on Unsplash

Just imagine if someone stole your phone. If everything is super convenient, the criminal would only need to crack the password, and they’ll have access to your entire digital life. Well, to make things even worse, cybercriminals don’t need to touch your phone. They can breach your device on a public network while you’re sipping on an ice latte. And the dangers don’t stop there. In fact, they’re only just beginning.

AI threats

Cybercriminals welcomed AI with open arms. As soon as ChatGPT broke into the mainstream, bad actors started using it for data poisoning, launching successful attacks, and damaging systems. Hackers around the world use machine learning algorithms to improve their scamming strategies, breach systems, and automate their tedious tasks.

The numbers are staggering. Due to the popularity of ChatGPT, there was a 1265% increase in phishing emails last year. This makes AI a force to be reckoned with in the cybersecurity niche. But it’s not all bad. Experts are figuring out ways to add traditional cybersecurity methods to defend against attacks and even initiate predictive measures to avoid such

threats in the future.

Advanced phishing attacks

The weakest link in every cybersecurity system is a human. Why breach the castle when you can enter through the back door? Cybercriminals use the best strategy: socially engineered attacks directed at our emotions. And it works every time! What's worse, thanks to large language models (LLMs), they will keep working even better. Hackers can use a prompt to craft a perfect message, clone a profile, and create malicious code in seconds.

Multi-factor authentication isn't as secure as you think

After a decade, multi-factor authentication (MFA) is getting the love it deserves. But mass adoption might be coming a bit too late. EvilProxy abused fake login pages and stole MFA tokens in 2023. And they did it quite successfully by exploiting Indeed to steal Microsoft accounts.

Of course, every public login system needs to have MFA protection, but MFA fatigue plays a factor and opens the door for cybercriminals. Make sure your team knows about it. Another thing that opens the door for hackers is a DNS leak, which can happen even when using a VPN. Perform a routine DNS leak test to ensure requests aren't revealed, and check up on every cybersecurity tool you use.

Geopolitical threats

The world is in chaos. Ukraine and Russia are at war. Israel and Palestine are at war. But modern wars aren't fought only with guns and bombs. They're fought with information. Cyberattacks, fake news, and deepfakes can create conflict in

a matter of minutes.

This year will be plagued by many elections, conflicts, and the 2024 Summer Olympics. The last time the Olympics aired, there were 450 million cyberattacks on its infrastructure. Social media platforms will be used again to promote unchecked campaigns. The head of security policy at Meta, Nathaniel Gleicher, stated that their platforms have been used to run foreign interference campaigns. But they don't know when a campaign is coming, which can happen at the last minute. So don't believe anything you see online.

How To Keep Up With The Latest Cybersecurity Trends

Being up to date with the latest cybersecurity trends can be daunting if you know very little about the topic. That's where these suggestions can help you out:

- **Read reputable publications:** Blogs, journals, magazines, and newsletters compile the most important data into 5-minute reads. Some of the best are The Hacker News and Beeping Computer.
- **Follow cybersecurity experts on social media:** Nowadays, there's an influencer for everything, even cybersecurity. Dave Kennedy, Chris Krebs, Brian Krebs, and Rachel Tobac are some of the best. The more cybersecurity tips you see on your timeline, the faster the information will stick, and the better you'll be at applying best practices.
- **Listen to podcasts:** Do you have to commute for more than 15 minutes a day? If so, tune into some podcasts like Darknet Diaries, The CyberWire, and Security Now to learn something new. You'll be surprised at how much you can learn by devoting a quarter of an hour to listening to cybersecurity podcasts while driving between places.

- **Watch online courses:** Udemy, Coursera, and even YouTube can serve as a starting point for learning more about cybersecurity. You'll gain knowledge and a credential to add to your resume. With time, you can take on the responsibility of being the cybersecurity guru at your office and protecting everyone's data!
- **Join a community:** Reddit's r/cybersecurity, GitHub, and Stack Exchange are the most popular tech forums where you can start or join a conversation about a topic that interests you. You'll be surprised at how positive and helpful the members are.