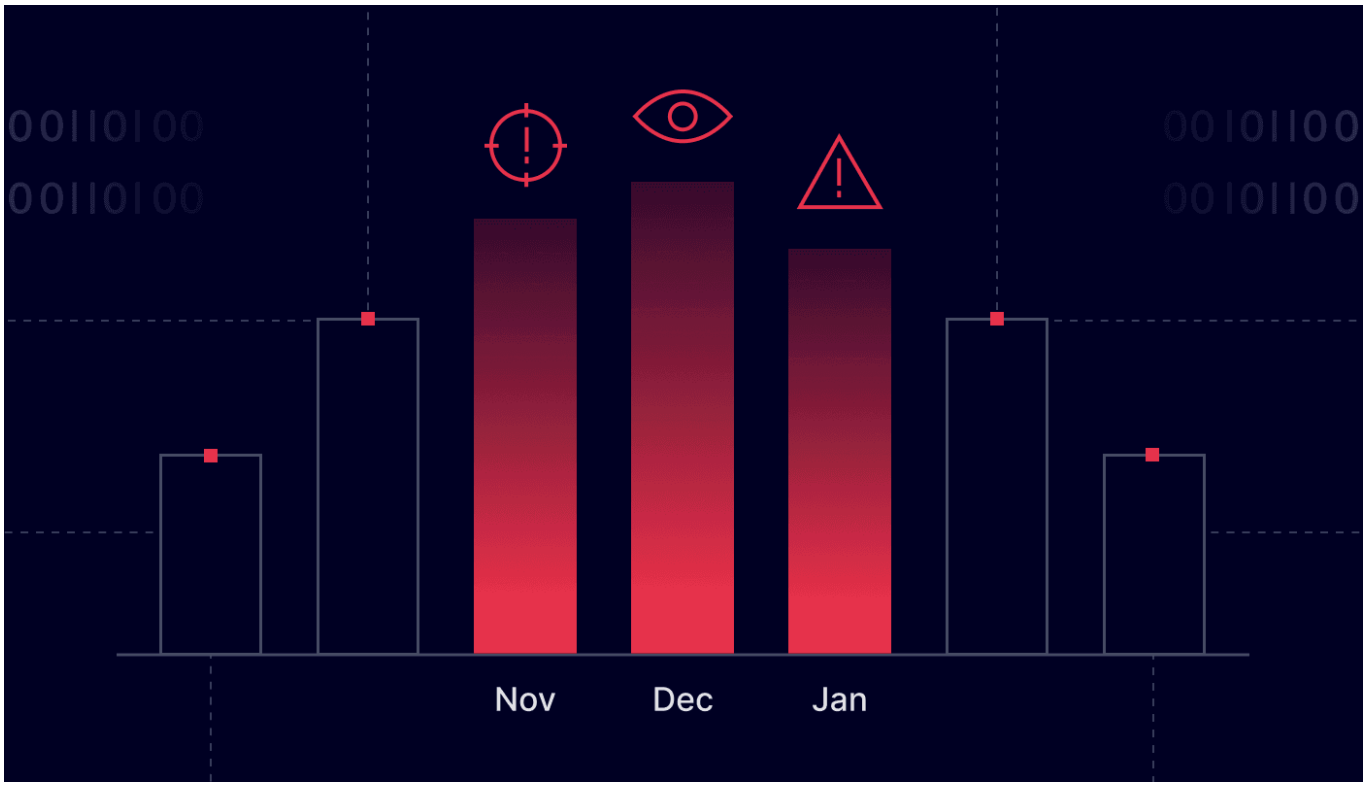
TRENDS & STATISTICS

The darkest season: the peak time of cyber threats

Anastasiya Novikava

Dec 3, 2024 7 min read



Summary: *Dark web forums peak in activity during winter months. Holiday scams surge, boredom rises, and AI makes cyber-attacks easier.*

The dark web is a key enabler for cybercrime. It allows bad actors to share tools, knowledge, and services secretly.

Anyone wanting to buy illegal items—like cyber-attack tools or drugs—can find them on dark web marketplaces. These markets appear and disappear quickly as they get blocked. They are usually advertised on dark web forums, and some even have mirror sites on the clear web.

Researching the dark web is hard because marketplaces have short lifespans. They come and go quickly. That's why NordLayer and NordStellar decided to analyze **dark web forums** instead.

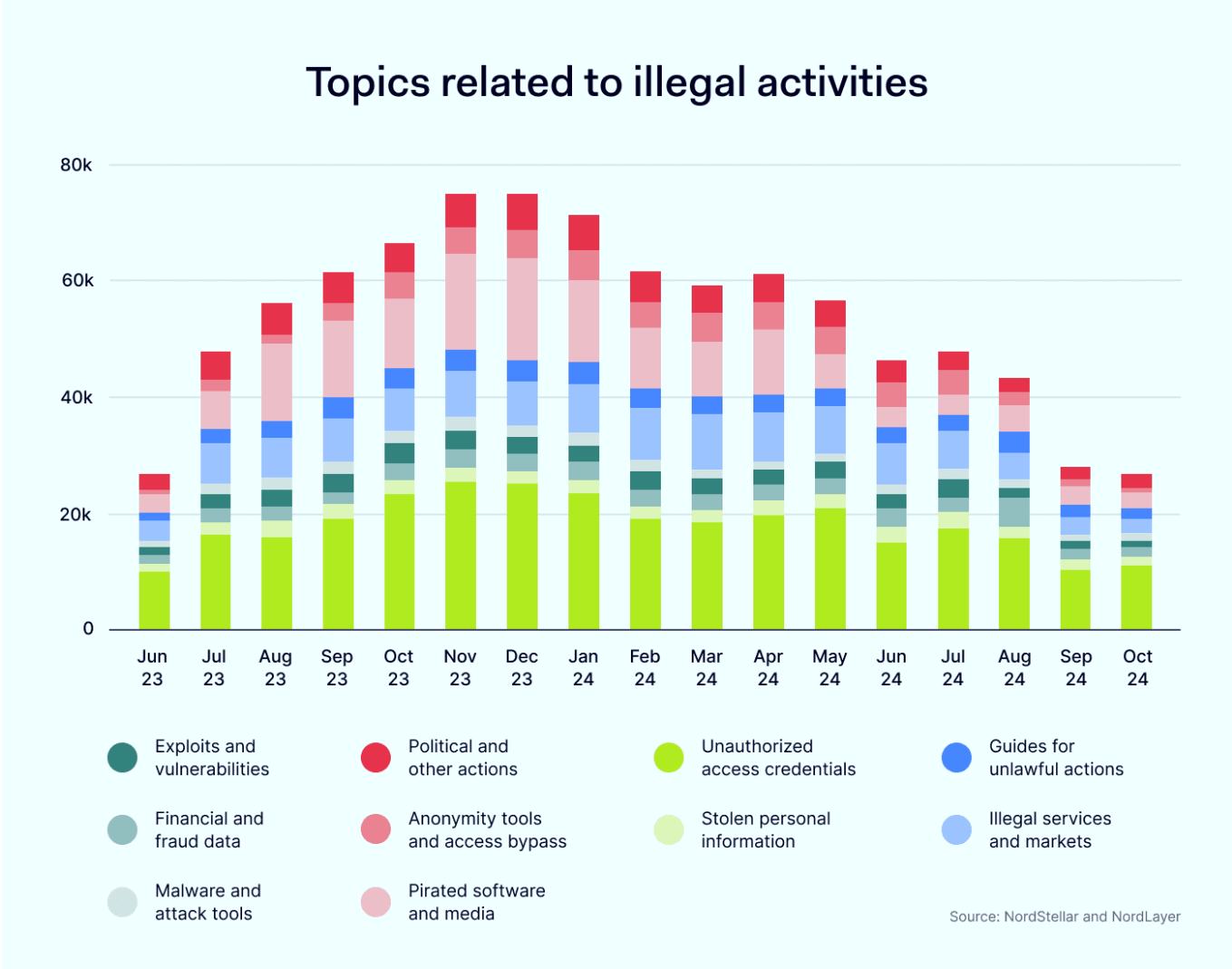
Forums are more stable over time. This stability makes it possible to see trends in discussions. These forums mix legal topics like news, politics, and content sharing with illegal activities.

However, legal activities like whistleblowing make up less than 1% of the content. Illegal activities are the largest part. By studying these forums, we wanted to uncover new trends in illicit activities.

Our research shows that **illicit posts peak in November, December, and January**. The darkest months of the year also see the most activity in the web's shadowy corners.

Why is winter the peak season for illicit posts?

We studied posts from June 2023 to October 2024. We categorized posts by topics and focused on illicit ones. Here's how those posts were distributed:



These numbers reflect posts on the dark web, not actual attacks. However, research by BitNinja Security, Cloud Security Alliance, and Mimecast shows that **Q4 is also when most cyber-attacks take place**. This suggests a link between increased dark web activity and real-world cybercrime during this period.

Why are threat actors more active in dark months, both discussing illicit topics and committing crimes?

> **Carlos Salas (Sr. R&D Engineer at NordLayer):** “In most industries, November to January is the busiest time, mainly because of the high amount of transactions from **Thanksgiving, Black Friday, and Christmas**. Criminals exploit this, knowing people are more likely to click on a phishing link while going through thousands of email orders and offers, compromising their network security.”

It's a known issue. Black Friday is already called Black Fraud Day. In the UK only, more than **16,000 reports of online shopping fraud** were recorded between November 2023 and January 2024, with each victim losing £695 on average.

> **Andrius Buinovskis (Head of Product at NordLayer):** “Everyone is looking for gifts and the best prices, and fake ads try to hook you into deals. Bad actors exploit this season, using **urgency tactics boosted by AI** to spread threats. People are more relaxed and less cautious, paying less attention to how they use personal and company devices. Employees might receive **phishing emails** like a supposed 'yearly bonus' from the CEO, which could lead to catastrophic consequences for the company.”

But on dark web forums, people discuss not only cybercrime. A big part of forums is about sharing **pirated software and media**, like movies.

This number grows in dark months. Comparing the summer months of 2023 with November—January, the number of dark forum posts about all kinds of pirated content **surged by 105%**.

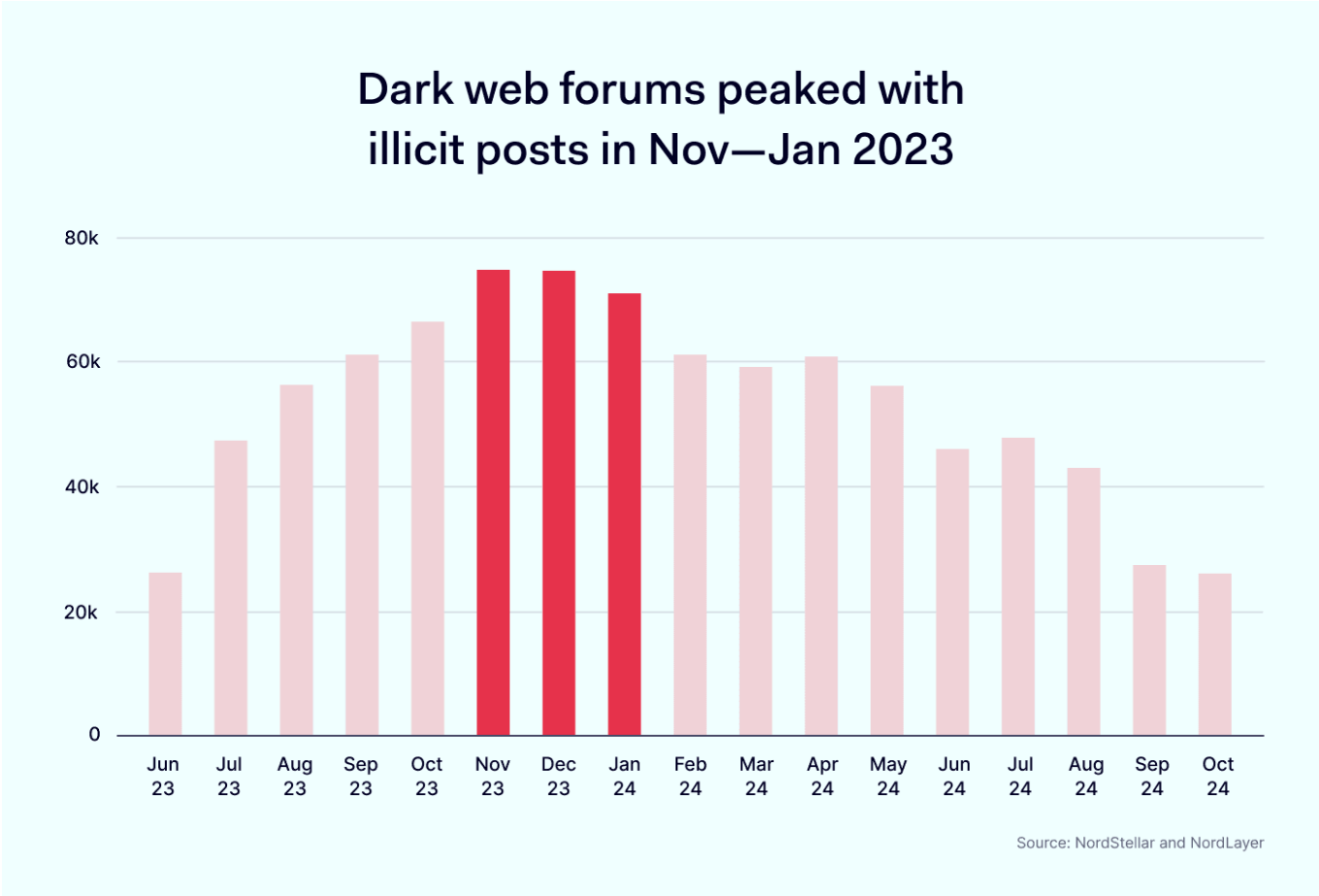
> **Vakaris Noreika (Head of Product at NordStellar)**: “I think it's the weather, to be honest. People tend to stay at home more and sit at their computers bored, which makes them more active in their cybercriminal activities. We've seen **a similar effect during the COVID lockdown** when the number of dark web users increased a lot. We also see fewer large data breaches in the summer, and this cycle seems to repeat every year.”

Like advanced persistent threats, “**advanced persistent teenagers**” are now a problem. Bored but skilled threat actors cause major disruptions. They trick employees with emails

and calls, posing as help desk staff. These attacks lead to data breaches affecting millions. **Teenagers now show techniques once limited to nation-states.**

Another factor is adding to the boredom of dark web forum users. They are mostly from countries where winter is pretty harsh. Most users accessing Tor—the browser used for dark web activities—are from **Germany** (36%), **the US** (14%), and **Finland** (4%). For countries where users access Tor via bridges, the top is **Russia** (41%). Maybe dark web forums are just the coziest winter hangouts.

Changing platforms and AI effects on cybercrime



Our research shows that September and October of 2024 had much fewer posts about illicit things on dark web forums than a year before. Why is that?

> **Vakaris Noreika**: “There could be many reasons why this happens. The most notable ones are maybe the platform changes; some hacker forums close, others open up,

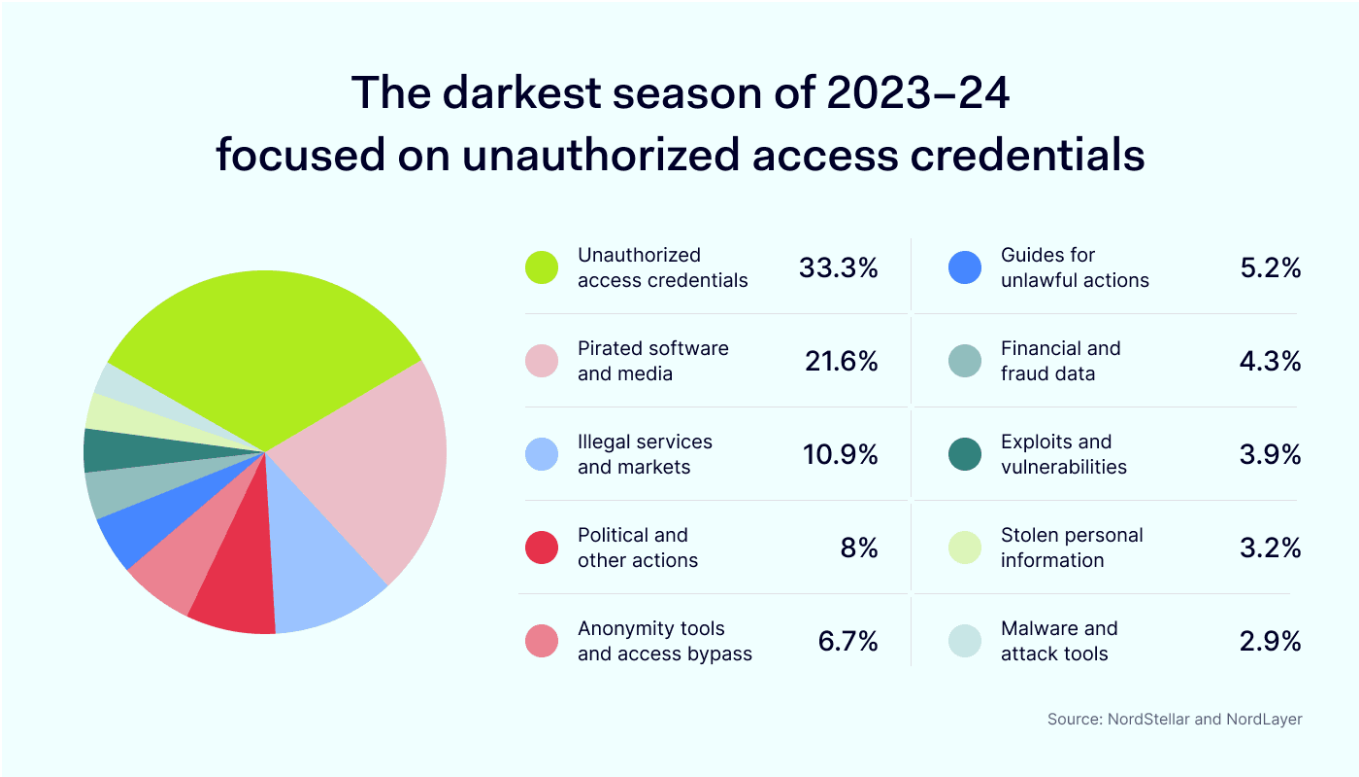
> some become popular to fade out later.
>
> There are some hacker communities, especially from Russia, which have been active for more than 20 years now. This is because the forum owners don't get arrested, unlike forum owners from the US, UK, etc., who do get arrested way more often.
>
> **Telegram** has also been a huge platform change. We've seen exponential growth in hacking-related activity on Telegram since the beginning of the war in Ukraine. But Telegram activity is focused on niche topics, while forums cover a wider range of ideas."

Another trend affecting dark web discussions could be **AI use in cybercrime**.

Retail and cloud computing giant Amazon, which can now view activity on around 25% of all IP addresses on the internet, says it is seeing **hundreds of millions more possible cyber threats** across the web each day compared to earlier this year. They used to see about 100 million hits per day, but that number has grown to **750 million** over six or seven months.

Amazon's Chief Information Security Officer is sure AI is making tasks easier for ordinary people, allowing them to do things they couldn't do before just by asking the computer. This might explain fewer discussions on dark web forums—why ask others when AI can do the work for you?

How to protect organizations during peak cybercrime seasons



So, winter months bring not only holidays but also heightened cyber risks. Instead of enjoying time with your family, you might find yourself dealing with cyber-attacks.

But don't worry—there are steps you can take to protect your organization. The good news is these measures aren't expensive or hard to implement.

Many of these precautions are the same as those needed year-round. Basic cybersecurity practices like employee training, strong passwords, and regular software updates are essential.

Employee education is the first line of defense.

> **Vakaris Noreika**: “It's hard to control what happens with your employees. **It's unavoidable that their data will be leaked online**, and this data might be used to attack your company. Here's what I always encourage companies to do:
>
> 1. **Educate employees** about phishing, credential stuffing, and other popular attack methods.
> 2. **Take care of the information that's already leaked**: monitor it and react. NordStellar can help with that.
> 3. **Manage access** to important company resources carefully.

> By doing this, you will be better off than 99% of companies around."

Prepare now to minimize risks during the peak cyber-attack season.

> **Carlos Salas:** "**Double down on cybersecurity awareness** in months before the high season. Consider having a pentest done beforehand to know what could be exploited by criminals.
>
> That said, we're humans, and there will always be a chance of clicking the wrong link or sharing the wrong files. So, practices such as **network segmentation**, **setting up security policies for devices**, or using toolsets such as **Data Loss Prevention suites** and **malware protection** are a must-have. They help contain the threats and minimize the 'blast radius' of any security incident."

With AI making cyber-attacks easier, it's crucial to think about these things right now, when the cyber-attack season is at its peak. The next year could bring even more advanced threats.

So, give your company a Christmas present and invest in a **solid cybersecurity solution**.

Methodology

NordStellar acquired data from over 80 forums where illicit activities are most often discussed. These forums span different web layers: the clear web, the deep web, and the dark web. We gathered textual content from forum threads between June 2023 and October 2024. The numbers we obtained represent the number of forum posts.

We used a fine-tuned AI model to categorize dark web posts into 67 tags. These tags were then grouped into 10 broader categories. For example, the tag "SERVICE" refers to posts where users offer services for a fee, including hacking or hiring hitmen. This tag falls under "Illicit services and marketplaces."

The study is thorough but has limitations from analyzing posts on approximately 80 forums only. Additionally, the shorter lifecycle of criminal sites and the rapid rise of mirror sites can affect data consistency and completeness.

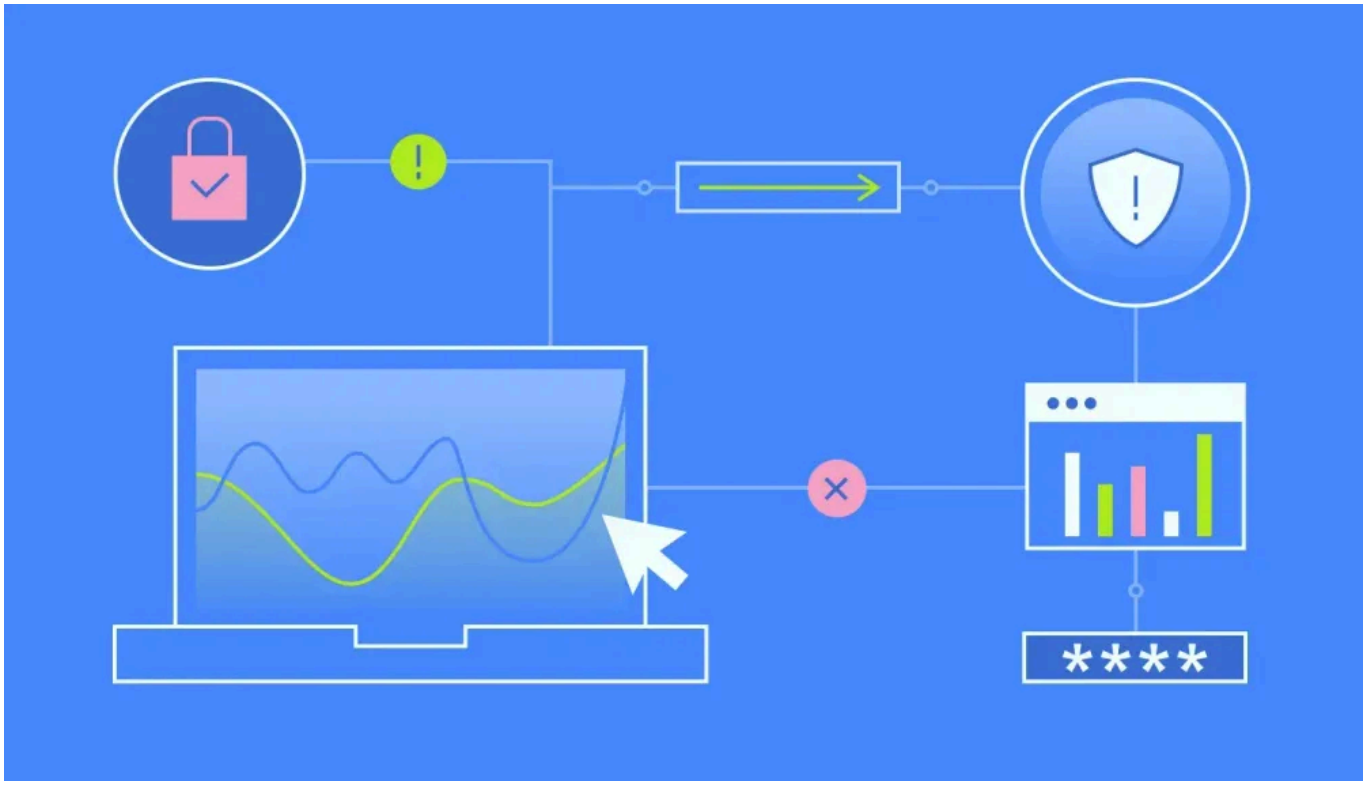
Anastasiya Novikava

Copywriter

Anastasiya believes cybersecurity should be easy to understand. She is particularly interested in studying nation-state cyber-attacks. Outside of work, she enjoys history, 1930s screwball comedies, and Eurodance music.

Share this post

Related Articles



TRENDS & STATISTICS