We've looked at several common cybersecurity vulnerabilities and the solutions to those. Today, we are keeping it simple, focusing on VPNs. A VPN is a tool easily accessible to home and business users and can provide a strong layer of security to your networks and devices.

Dr. Ronald Walcott
Managing Director

A virtual private network, or VPN, acts as a tunnel between you and your destination on the internet, encrypting everything inside.

For the average consumer, though, a VPN is a fantastic tool. It means you can access your files and media from any location, securely and privately.

PROTECTING YOUR PRIVACY

Privacy is not always a given when you're online. It's usually taken. Advertisers, social media networks, and apps routinely track who you are, what you're doing, and even where you live. If you search for a particular item on Amazon, you may start seeing ads for those items on Facebook. This is also true for physical locations, such as apartment rentals. A VPN makes it impossible to track location, obscuring it from advertisements. That obscured location makes it impossible for advertisers to serve ads based on your location. And, the profile that advertisers create – and we know they create profiles for every website you visit – will be incorrect. Your IP address won't match the location from where you are connecting to the ad networks and website owners.

That can be surprisingly freeing – you don't have to think about someone spying on your online activity or serving ads. You don't have to worry about anyone building a profile about you and what you like to do or the sites you want to visit. Of course, there are also benefits in terms of personal security because the VPN also encrypts the connection.

PROTECTING YOUR ANONYMITY

A VPN also protects your anonymity. This is a slightly different term than privacy. It means you are completely anonymous. When you visit websites or purchase products, when you stream movies or download television shows, it's one thing to be private because no one can track what you do.

No one can see what you are doing online (that's privacy), and no one will know who you are or where you live (anonymity). However, anonymity goes one step further. You are safe from being watched and tracked, but your identity is also secure.

Cookies used to track personally identifiable information won't know your location, and the VPN encrypts data transmission so that your ISP can't track it.

Overall, a VPN provides a level of security, privacy, and anonymity to make your web travels safer and give you the peace of mind that you are not being tracked.

In this Issue:

FOCUSING ON VPNS

HEADLINE NEWS: OKTA, MICROSOFT CONFIRM BREACHES CONNECTED TO LAPSUS$ HACK

UPCOMING EVENTS

VPNS DON'T LOG YOUR DATA OR ACTIVITY.

VPNs are also very safe because the majority of them don't log any of your data or activities. As mentioned earlier, VPN companies use shared IP addresses to give users anonymity online. However, this means that the company has no idea what you're doing on its servers, primarily if it operates a no-logs policy. This means that it's not collecting any personal information about you!

This is why most VPN companies guarantee 100% privacy with their services – every user can be anonymous on the web using a reliable VPN service provider.

SOME VPNS PROTECT USERS FROM MALICIOUS ACTIVITY

A handful of VPNs also come with built-in phishing protection and ad-blocking capabilities. This enables them to stop users from accessing potentially harmful websites containing phishing links or adware that could infect their devices.

Frequently Asked Questions:

CAN A VPN BE HACKED?
though using A vpn makes you secure, like all online things it can also be hacked, although the likelihood is highly reduced.

IS IT LEGAL TO USE A VPN?
Having a VPN can be beneficial depending on why you want to be invisible online. VPNs can protect you but can also be used to do something illegal on the internet. This is when you may get in trouble with the law.

HEADLINE NEWS:
Okta, Microsoft Confirm Breaches Connected to Lapsus$ Hack

Microsoft saw some of its source code released after Lapsus$ compromised an account, but it says that the code isn't sensitive. Okta says that attackers in January gained access to a support engineer's laptop for five days, which resulted in the exposure of data for some of its customers.
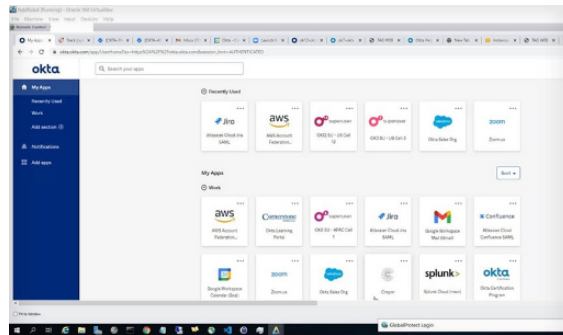
Lapsus$ has been behind a number of recent incidents, including supposed breaches of LG, Nvidia and Samsung.

On Tuesday, images allegedly stolen from Okta appeared on a Telegram page apparently run by Lapsus$. Subsequently, however, Lapsus$ revised the contents of the page to instead claim that "we did not access/steal any databases from Okta - our focus was only on Okta customers."

The crime group claimed to have gained "superuser/admin" access to multiple systems used by Okta.

Later in the day on Tuesday, Okta released an updated statement, saying about 2.5% of its customers may have been affected but did not give a precise figure. It said the data of those customers "may have been viewed or acted upon."

The Okta breach has raised alarm across the security community. Okta's authentication and identity management software is widely used by enterprises. Some have called on Okta to be more transparent about the incident and its possible effects.

Source: https://databreachtoday.com

Upcoming Events

CLOUD DATA SECURITY SUMMIT
March 29, 2022

UKI CYBERSECURITY SUMMIT
May 24, 2022