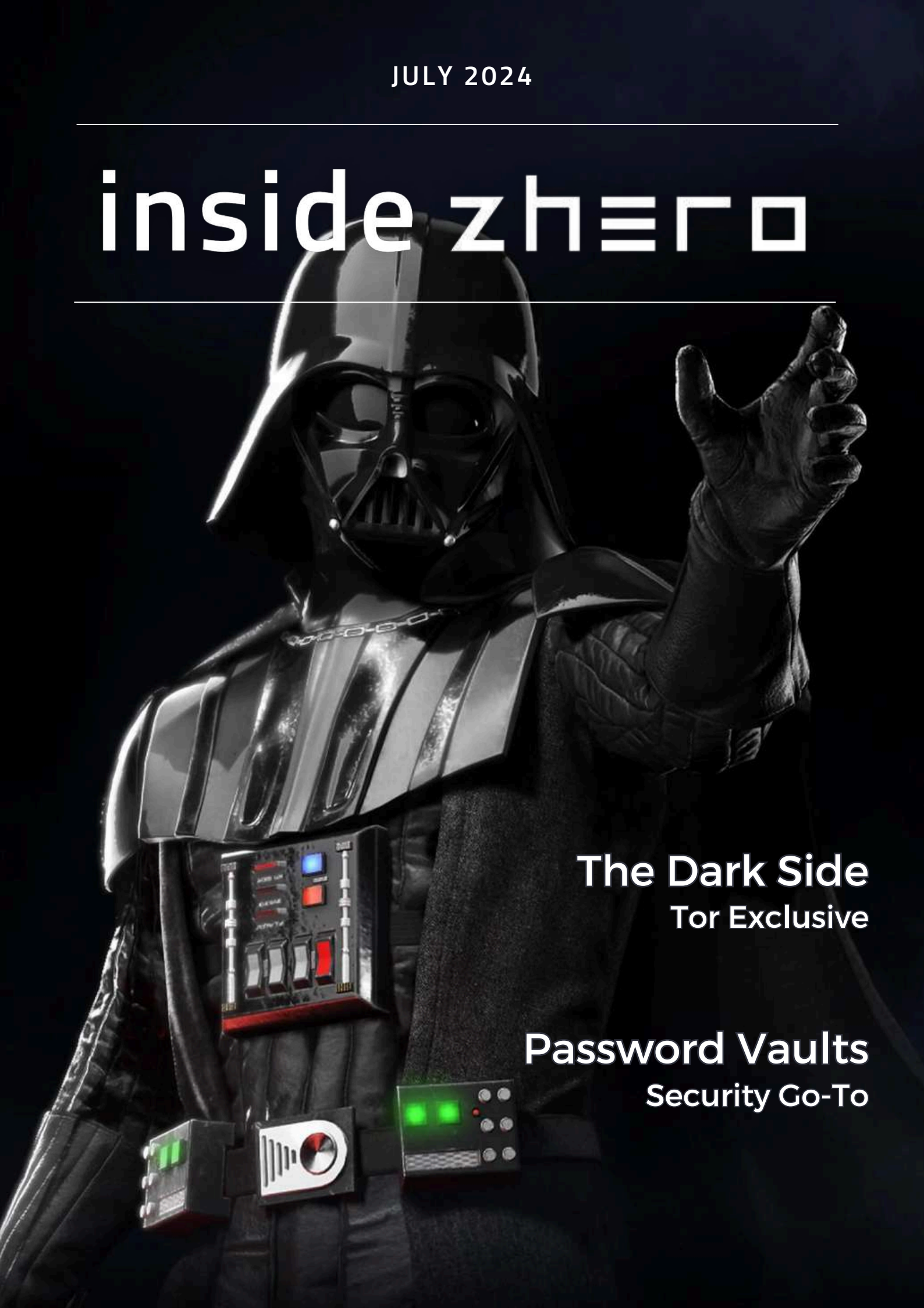
JULY 2024

inside zhero



The Dark Side
Tor Exclusive

Password Vaults
Security Go-To

Message from Izak

Greetings, and a warm welcome to this edition of Inside Zhero. Despite the Euro 2024 result, we're all still smiling.

This month we're focusing on the Dark Web – its ugly, not so dark, and useful sides.

IZAK OOSTHUIZEN
Chief Executive Officer,
Bestselling Author

In this issue

Our feature "The Dark Side" takes a look at the origins of the Dark Web, what it's used for and who uses it.

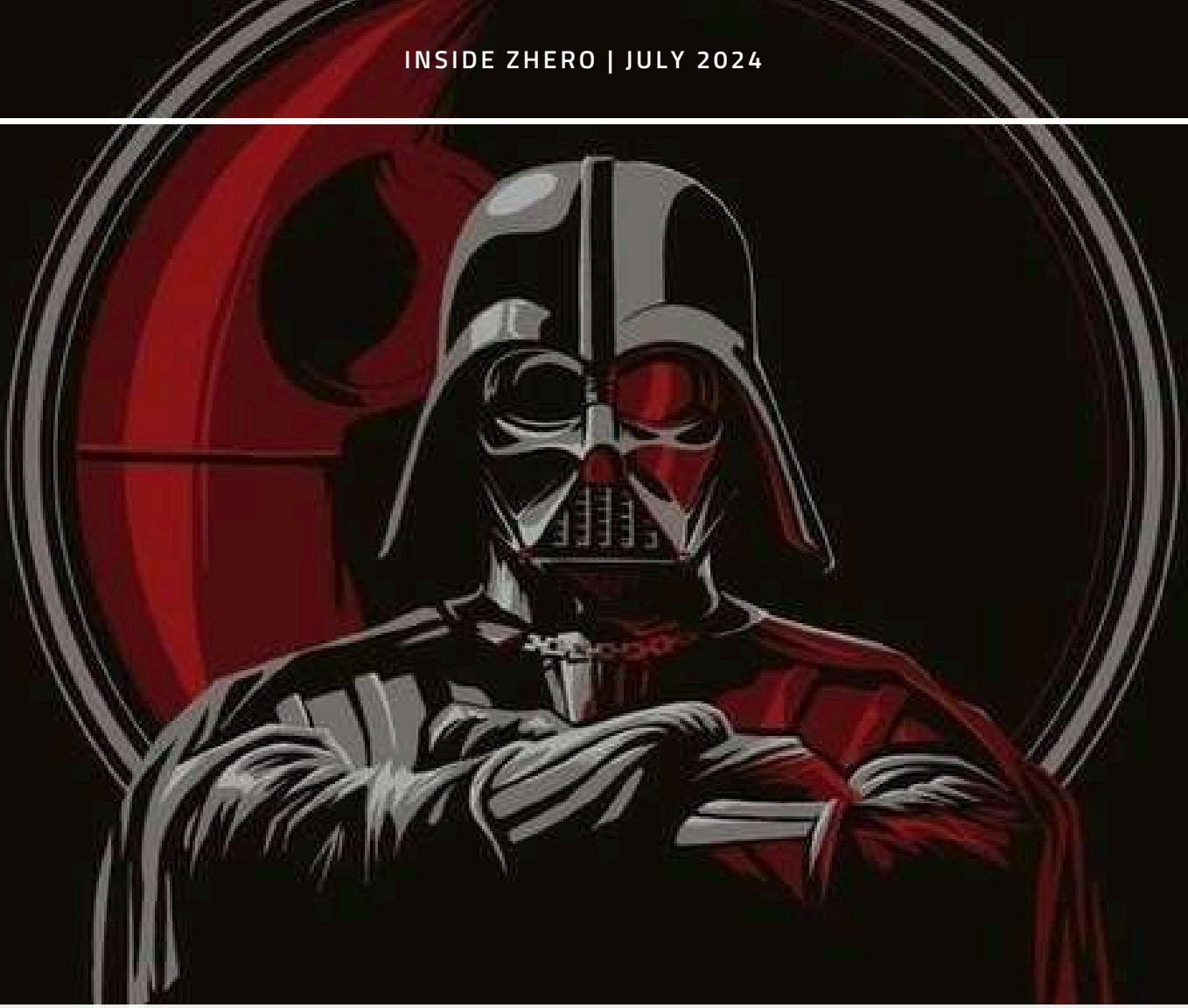
The Dark Web has about 2.7 million daily users of whom 2% are from the UK.

“In the absence of oversight and authority, and with a sense of anonymity, the Dark Web lures renegades and cybercriminals who defy conventional authority and exploit the uncharted digital landscape for personal gain. I think it's a lot like the infamous outlaws of the Wild West."

Izak Oosthuizen

Zhero Founder and CEO,
Bestselling Author

Available Now



THE DARK **SIDE**

When we conjure up thoughts of the Dark Web, evil, crime and corruption probably spring to mind. Almost 57% of the content is indeed illegal and violence, extremist platforms, illicit marketplaces, drugs and cybercrime forums abound. Also, most serious hacks take place via the Dark Web, costing more than £7 million in the United States. DDoS (Distributed-denial-of-service) and malware attacks are part of a thriving market on the Dark Web and a threat actor can buy 1,000 threat installs for £1,500. But it's not all bad. The Dark Web was born out of good intentions and continues to have legitimate users. Let’s explore how it all began and developed to become the global cybercrime giant it is today, valued at $9 trillion.

The Dark Web

Most of us access the internet through popular web browsers like Google Chrome, Safari, and Edge. However, there are deeper levels of the internet that are not accessible to the average user. The Dark Web is a collection of websites, forums, and marketplaces that can only be accessed using the Tor browser. This specialised browser provides a level of anonymity that is particularly appealing to cybercriminals, hackers, and government operatives who wish to conceal their identities. The Dark Web forms only part of the internet which is also made up of the Surface web and the Deep Web.

The Surface Web

A lot of the time we only interact with the visible or "surface web," which consists of nearly two billion public websites accessible through search engines. Sometimes called “Clearnet”, this part of the internet includes sites like Wikipedia, public sector websites, news sites, YouTube videos, blogs, Instagram, and much more. However, the surface web is just the tip of the iceberg, comprising only about 4% of the entire web. The majority of web pages remain hidden from the average user. Why is this the case? Because not all information available online is meant for the public domain.

The Deep Web

Most of the digital content in the world is not accessible via web search engines. This vast amount of information resides on the Deep Web, where most online activities occur. You use the Deep Web as part of your daily routine. Whenever you log into your email account, check your online banking details, or use social media, you're accessing the Deep Web. The Deep Web contains information that typically requires a username and password to access, primarily for security and privacy reasons. The Deep Web also includes databases, social media apps, forums, and paywall-protected content. The Deep Web and the Dark Web make up 96% of the internet.

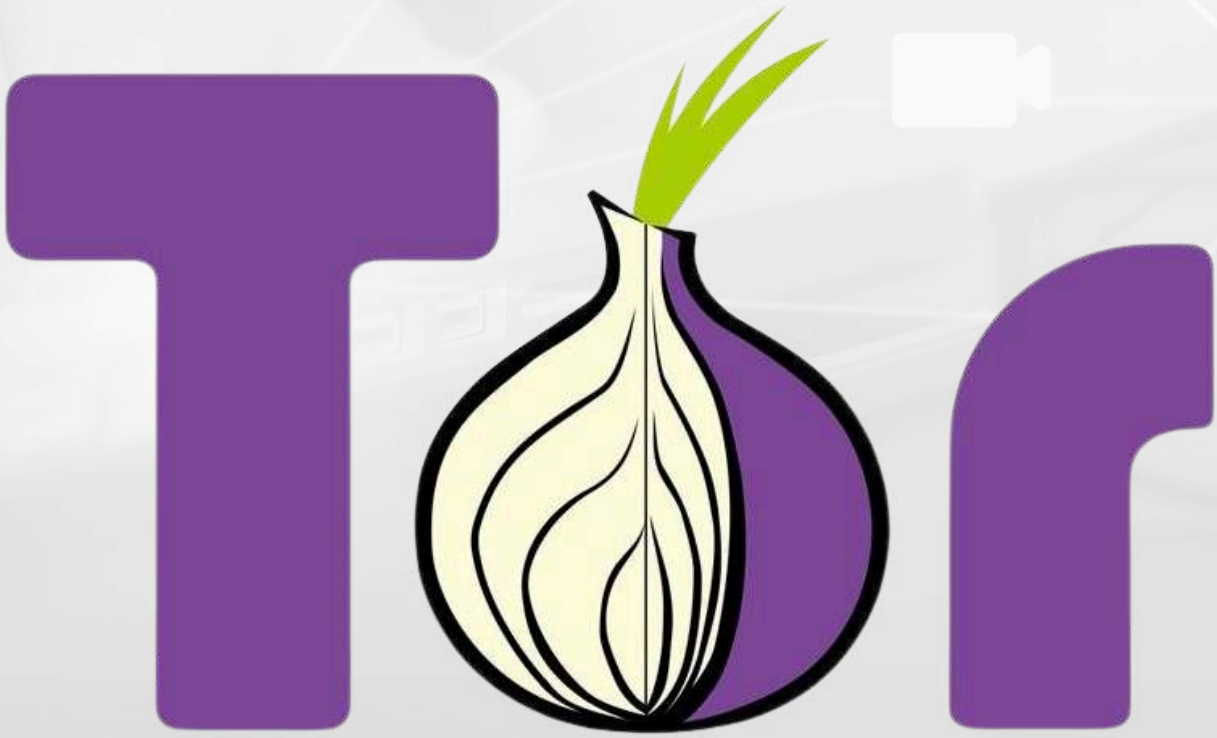
Started Light

While the origins of the Dark Web are unclear, it's often talked about in tech and digital security circles as a hotspot for many security issues. The Dark Web runs on a network of nodes and systems called "darknets." This includes peer-to-peer networks, both small and large, like Tor and Freenet. The Dark Web started out light. One of Tor’s original uses was to hide the communications and identities of American operatives and dissidents living within oppressive regimes overseas. Freenet’s original purpose was freedom of speech and combatting censorship. This tradition continues to this day, with Dark Web services such as SecureDrop to upload sensitive documents, and Ricochet Refresh for secure chat. To browse the Dark Web, you need special software like the Tor browser. Since it plays a big role in online activity, it's worth understanding how this Dark Web browser works and why it's used.

Tor Browser

Developed in the mid-1990s to protect U.S. intelligence communications, the Tor Project is now the go-to method for accessing Dark Web content. Tor, short for The Onion Router, uses three layers of encryption and a unique routing mechanism to ensure complete anonymity. It combines robust encryption with the ability to route internet traffic through a network of relays randomly.

This high barrier to entry exists to protect user identities, online activities, and locations, ensuring anonymity. Using the Tor browser, users can access the Dark Web to communicate and share data confidentially, without the risk of being traced. Most Dark Web users also log into a Virtual Private Network (VPN) to further conceal their identity.



Dark Web Today

Today, there are over 65,000 unique .onion URLs on the Tor network. About 10% of these sites support communication via forums, chat rooms, file hosts, and marketplaces, serving legal and legitimate purposes in free societies. In repressive regimes, the dark web provides a lifeline by offering access to information and protecting individuals from persecution. In freer societies, it serves as a critical tool for whistle-blowing and secure communication, shielding users from repercussions. Major organizations like newspapers, Facebook, and even the CIA maintain Tor hidden services to facilitate anonymous communication for sensitive information, emphasizing their commitment to privacy.

Springboard for crime

On the other hand, while privacy and anonymity can shield people from tyrants and targeted ads, they also make the dark web a hotspot for crime. This includes arms trafficking, drug dealing, and sharing exploitative content, often involving children, like pornography and violent images. It's also a platform for websites promoting the views of neo-Nazis, white supremacists, and other extremist groups. It’s this dark side of the Dark Web that is worrying, particularly the products and services sold on marketplace forums.

What's for sale?

The pairing of Dark Web services with cryptocurrencies has led to a boom in online crime. Put simply, the combination of a secret encrypted network and a currency that's hard to trace by law enforcement has led to a small but significant marketplace. Here, shady vendors sell illegal goods and services without much worry about getting caught. Some of the illicit products that scammers peddle on these black markets include stolen and counterfeit data which comes in many varieties including personal data, financial data, online account login data, medical data, confidential corporate data and forged data, most notably fake passports.

A cybercriminal can purchase the details of a credit card with a £4,000 balance for only £85. A false passport costs upwards of £5,000. The Dark Web is also a hotspot for money laundering, enabling crooks to disseminate the money that they steal, extort, or otherwise take from their victims and turn it into clean, untraceable cash.

Cybersecurity risks

Besides selling personal data and compromised accounts on the Dark Web, cybercriminals also sell:

- **Exploits** - Off-the-shelf software kits used by cybercriminals to attack system vulnerabilities and distribute malware.
- **Malicious Software** - Includes ransomware, information stealers, keyloggers, spyware, adware, rootkits, Trojans, and worms with self-replicating capabilities.
- **Malware-as-a-Service (MaaS)** - Subscription-based model providing cybercriminals with tools, software, distribution networks, targets, technical support, and management dashboards.
- **Software Vulnerabilities** - Zero-day exploits that allow cybercriminals to infiltrate systems undetected, exploiting unknown weaknesses in software.
- **Botnets** - Networks of compromised devices providing computing resources for cyberattacks.
- **Distributed Denial of Service (DDoS)** - Services that utilise botnets to overwhelm victims' systems with traffic, knocking them offline.
- **Cybercriminal Training** - Tutorials, guides, and educational content supporting the development of malicious skills and techniques.

Can I access it?

The Dark Web isn't illegal and you can access it by downloading and installing the Tor browser. As many as 70% of users claim to use the Tor browser for anonymity, 62% said they use it for additional security, and 27% used it out of curiosity about the Dark Web. Only about 6.7% of global users use the Dark Web for malicious purposes, but it's smart to be selective about the websites you access. So, it's important to look before you leap.

Be sure to educate yourself on the potential risks and dangers. Make sure you install and run strong security software on your computer and devices to help ensure the privacy and security of your data.

At your own risk!

If you decide to access the Dark Web, here are a few safety and security issues to consider:

- **Criminals** - Be wary of shady websites run by criminals on the dark web. They sell illegal goods and may try to scam or steal from you.
- **Breaking the Law** - Engaging in illegal activities on the dark web can land you in serious trouble. Stick to legal and safe practices.
- **Suspicious Links** - Clicking on links could lead you to unwanted content or infect your device with harmful malware. Exercise caution and avoid downloading from questionable sources.
- **Law Enforcement** - Police also operate on the dark web to catch criminals. They work undercover like everyone else there.
- **Viruses** - Some sites may attempt to infect your devices with viruses. Avoid downloading anything from sites you don't trust.
- **Hackers** - Hacker forums exist where individuals offer illegal hacking services. Be careful as these individuals may target your devices.
- **Webcam Hijacking** - Beware of sites trying to install Remote Administration Tools (RATs) on your device. Cover your webcam when not in use to prevent unauthorised access.

"The dark net is a world of power and freedom: of expression, of creativity, of information, of ideas. Power and freedom endow our creative and our destructive faculties. The dark net magnifies both, making it easier to explore every desire, to act on every dark impulse, to indulge every neurosis."

Izak Oosthuizen
Founder & CEO, Bestselling Author

Protect yourself!

For businesses or individuals keeping an eye on the Dark Web, the old-fashioned methods of tracking are often slow and not very effective. Luckily, we're in an age where technology can step in and help out. Here are some tools and practices that businesses can use to stay ahead of cybercriminals lurking on the Dark Web:

- **Dark Web Surveillance** - Using tools that monitor the dark web is key. They keep scanning constantly for any leaked or stolen credentials. When a breach is detected, companies can quickly prompt users to change their passwords, cutting down the time cybercriminals have to exploit stolen data.
- **Employee Awareness and Training** - Making sure your team knows their stuff about cybersecurity is crucial. Training them on safe internet practices, how to manage passwords well, and how to spot phishing scams can beef up your overall defence.
- **Strong Infrastructure** - Businesses should invest in solid defences like secure VPNs, good antivirus software, and strong firewalls. These tools create a sturdy barrier against cyber threats.
- **Incident Response Planning** - Having a plan in place for when a data breach happens can soften the blow. It's about having clear steps to follow when there's a security incident, so you can act fast and minimize the damage.

SELF-ISOLATE
YOUR PASSWORDS TOO

Password vaults, aka password managers or password lockers, is software designed to store usernames and passwords for several accounts securely. These credentials are encrypted for protection. Users can access all stored information using a single "master" password.

This system promotes using complex passwords, as you only need to remember one master password, reducing the risk of stolen or compromised passwords. People in the know think of password vaults as a security go-to.

Minimise the risk

All over the world, people still use weak passwords or reuse the same password across multiple accounts. This enable cybercriminals to steal passwords and easily breach networks. Passwords with privileged access are particularly attractive to cybercriminals, as they can use this single “key” to access numerous resources for malicious purposes. The risks of such attacks increase when organisations don’t properly manage their passwords. A password vault is one way for companies and individuals to minimise the risk of password-based cyberattacks. Password vaults also provide superior protection again Dark Web intrusions.

Big benefits

- One password to rule them
- Generate random
- Simple access to multiple
- Easily change your passwords
- Use the autofill feature
- Share passwords securely
- Store other online credentials
- Use the same password manager across multiple devices
- You take IT security seriously

Which one for me?

There are a plethora of password vault vendors to choose from. In 2024, these are thought to be five of the best: NordPass, 1Password, Dashlane, Bitdefender PM and your old favourite, Norton. All are quite affordable, with NordPass costing only £1.79 per user per month. This goes up to £6.19 per user per month for 1Password, which includes a Dark Web scanner. Before you decide, shop around, think about the features you need and ask an IT guru for their advice.

ALAN ACES IT

At Zhero, we use KPIs as a benchmark to measure our performance, align goals, ensure accountability, drive improvement and much more. Ensuring our weekly KPIs are met, particularly those relating to Service Desk tickets, calls and ratings is crucial for us to deliver superlative customer service and productivity.

Our Service Desk Team are all exceptional at meeting KPIs, answering calls, closing tickets and getting 5-star ratings. In the last six months, however, Alan Ntini, one of our amazing Service Desk Engineers, has proven to be a formidable colleague.

Alan has received 24 5-star ratings, closed an incredible 1,064 tickets and handled an astonishing 3,213 calls. He is the Service Desk's Overall Performer this time round. Well done, Alan and congratulations on your outstanding achievement and a well-deserved incentive!

CRUSH IT CHAOS

Tune in here:

zhero | PODCAST

Meet the team

Macwhill Hanse

STUDENT DEVELOPER

Hi Macwhill! What made you realise you want to go into the IT industry?

My brother got me interested in computers. I wasn't interested in the hardware side but I really find programming cool and interesting.

What's your most-used productivity tool?

Microsoft OneNote to keep track of things every day.

How would you describe yourself?

I'm diligent, ambitious and hardworking. I think I get on well with people.

What do you enjoy the most about your role?

I love helping people solve their problems and making their lives easier.

Do you have any hidden talents or hobbies?

I like playing hockey and tennis. I also enjoying reading and gaming.

What is your favourite movie or TV show?

My favourite movie is The Theory of Everything. Stephen Hawking is still one of my role models.

LONDON
162 Farringdon Road
London
EC1R 3AS

SPEAK TO US
+44 20 7183 3975

zhero
crush the chaos