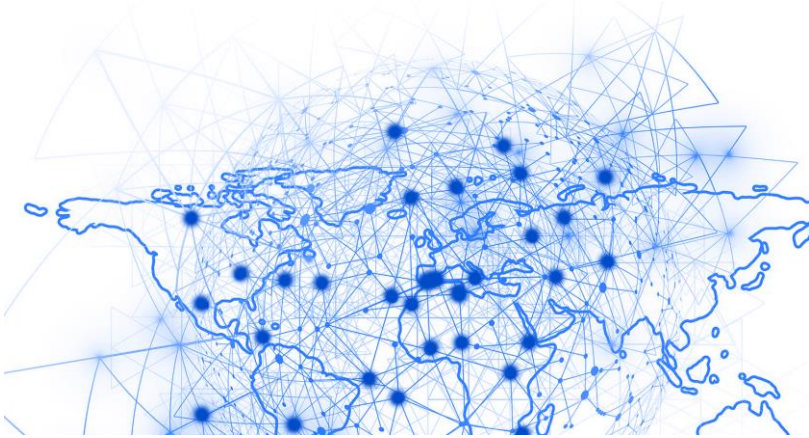
The Dark Side Of The Internet

YOUR IT DEPARTMENT

THE ORIGINAL STAR WARS SAGA HAS REACHED ITS CLOSE, BUT THE LOOMING THREAT OF THE "DARK SIDE" REMAINS SEARED INTO OUR CONSCIOUSNESS. THE DARK WEB MAY BE LESSER KNOWN, BUT IT'S A POPULAR PLACE FOR CRIMINAL ACTIVITY. **THIS EBOOK EXPLORES THE DARK WEB, ITS POSSIBLE IMPACT ON YOUR BUSINESS, AND WAYS TO REDUCE YOUR RISK EXPOSURE.**



WHAT IS **THE DARK WEB?**

Like the Dark Side in the Force, the Dark Web attracts the bad guys.

Continuing with Star Wars a little longer, think of the Dark Web as where Jabba the Hut and his bounty hunters would sell their ill-gotten gains. On the Dark Web, cybercriminals could be hawking important, sensitive, or proprietary business data.

THE US GOVERNMENT CREATED THE DARK WEB'S MULTI-LAYERED TOR (THE ONION ROUTER) TECHNOLOGY IN THE MID-1990S TO ALLOW SPIES TO ANONYMOUSLY EXCHANGE INFORMATION.

Not all Dark Web traffic is criminal. It is also visited by journalists and law enforcement agencies and is used in countries prohibiting open communication.

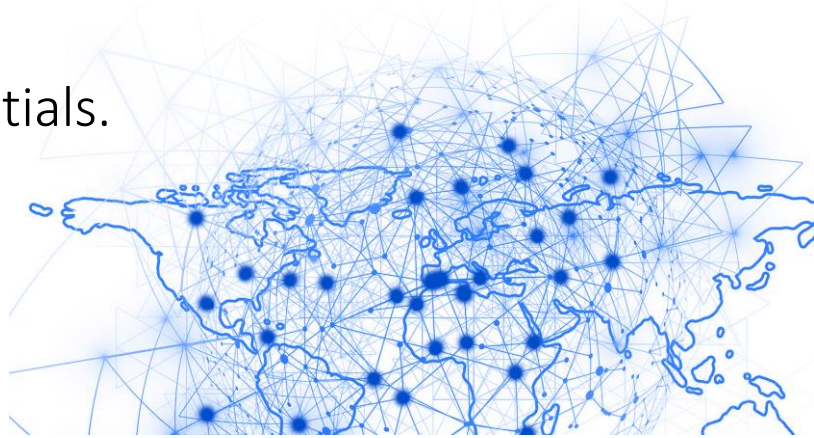
Still, it is a popular place for bad guys, because it isn't something you can find on your typical browser: you're not going to just type "darkweb.com" into

your Safari, Chrome, Firefox, or Edge browser. On the Dark Web, users access Web pages hidden from search engines.

Users need specific software, configurations, or authorisation to access the Dark Web. Users hide their IP address and use encryption to anonymise their identity for maximum privacy.

So, you'll find a lot of illegal activity on the Dark Web. Once users get in, they can buy all kinds of shady stuff:

- stolen credit card or bank account numbers;
- guns and other weapons;
- child pornography;
- counterfeit money.
- And the biggest threats to businesses:
- malware and tools to breach cybersecurity;
- leaked data;
- stolen access credentials.

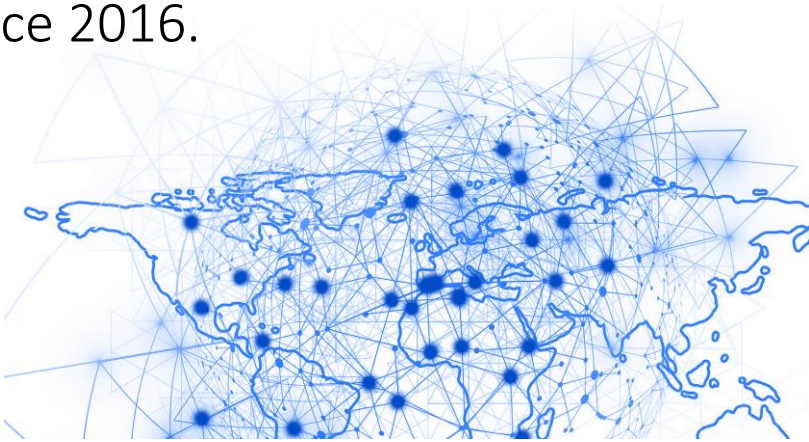


WHY SHOULD YOUR **BUSINESS CARE?**

Quite simply, your employees' usernames and passwords to access your business systems could be sold on the Dark Web. Or the leaked data could be the personal information of your customers, clients, or staff. A hacker who breaches your network and accesses proprietary information could put your secret sauce or new product innovation up for sale to the highest bidder.

Because it's being done on the Dark Web, your business wouldn't even know about it until the damage was already done.

One 2019 research study found that 60% of all listings on the Dark Web could harm enterprises. The number of those bad-for-business Dark Web listings had also risen by 20% since 2016.

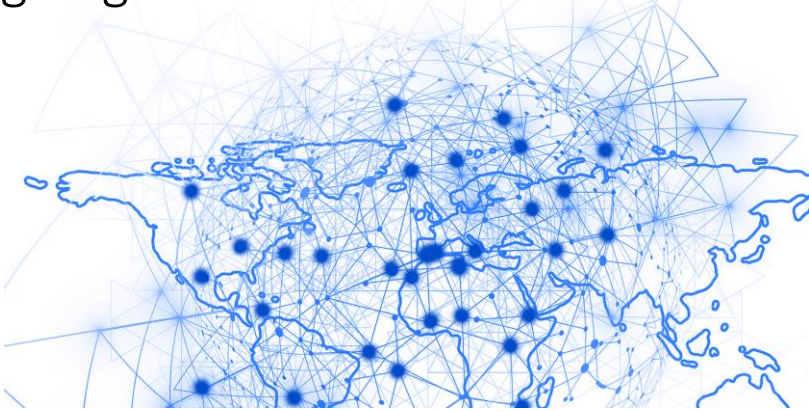


These Dark Web listings posed business risks such as:

- undermining brand reputation;
- loss of competitive advantage;
- denial of service attack or malware disruption;
- IP theft;
- raudulent activity.

IT COULD HAPPEN **TO YOUR BUSINESS**

You might think your business is safe. You've got top-notch firewalls and antivirus protection in place, but that's just the beginning. Perhaps you're too small or unsexy for a cybercriminal to care about your data, but your business doesn't even have to be breached to be at risk from what's going on in the Dark Web.



We often read about large enterprises suffering cyberattacks: big names such as Tesco and Easyjet have been hit. Now, you might think you don't care if someone buys a pilfered list of usernames and passwords for MySpace. Is anyone even on there anymore? But if you use those same access credentials for another account currently, your business could be at risk. The same is true of any of your employees found in the MySpace database.

Hackers rely on our tendency to repeat credentials and test out usernames and passwords from one account on others. They have the tools to easily enter the credentials en masse on business, domain registration, and Web hosting sites to see if they're in luck.

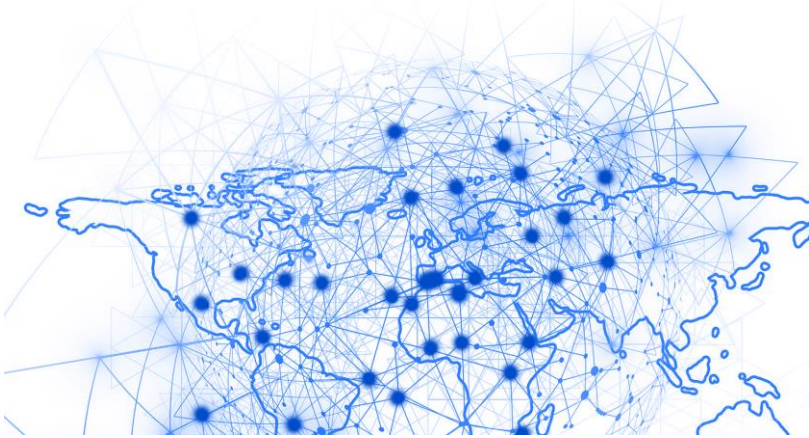
And breaches you don't even know about could be putting your business data at risk. A vendor you work with may not even know they've been targeted. But

already their database is available on the Dark Web for a few hundred bucks, and it just so happens to contain the confidential marketing campaign plan you sent their way!

Privacy specialists told a Federal Trade Commission conference that Dark Web victims included medical practices, retailers, school districts, restaurant chains, and other small businesses.

Worse still, Dark Web information is up to twenty times more likely to come from an unreported breach.

So, despite your best efforts, you could still be at risk? That's depressing, but don't give up. There are several strategies you can adopt to minimize threats.

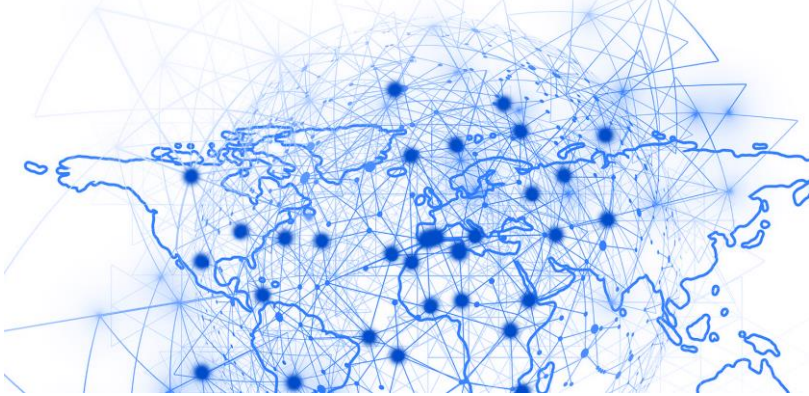


PROTECTING YOUR BUSINESS FROM **DARK WEB EXPOSURE**

The first step is to implement strong cybersecurity procedures. Be proactive. By the time your information ends up on the Dark Web, there's little you can do. So, maintain current security protection, install security patches regularly, and keep antivirus software up to date.

Limit users to access privileges dictated by their responsibilities. For example, someone on the marketing team probably doesn't need to be able to get into the HR database. So, don't give them those rights.

When people change roles, their access rights should, too. If someone leaves your organization, be sure to remove their privileges. Letting Jamie from accounting's old account sit dormant for decades

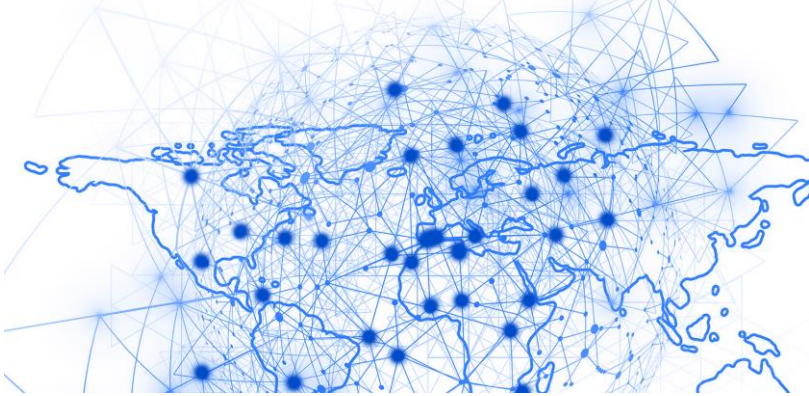


could be a real risk (especially if Jamie was big into MySpace back in the day!).

It's also important to educate your employees about cybersecurity best practices. These include:

- avoiding credential reuse – encourage them to use password managers to store random, hard-to-remember passwords;
- encrypting any mobile devices used for business purposes;
- accessing business networks using secured internet access points and approved devices only;
- questioning social engineering tactics, including emails with malware attachments or links to false sites.

Your business might also sign up for monitoring, which keeps an eye on the Dark Web for any data related to your business.

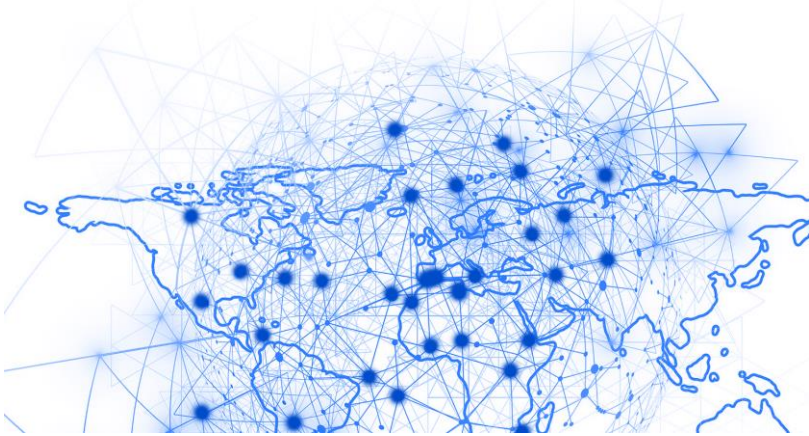


WE **CAN HELP**

Let a managed service provider be your Jedi Knight. We may not have a lightsabre at our disposal to fend off cybercriminals, but we have the tools to provide:

- Dark Web monitoring (to see if your businesses credentials show up on there);
- password management;
- user access management;
- data encryption;
- email security.

Our experts can boost your cybersecurity protection and set up Dark Web monitoring. Know that you're protected 24/7 with an IT team dedicated to ensuring your business data is secure from any Death Star-like vulnerabilities that lead to disaster.



Your IT Department

Unit 8 Farrington Way
Eastwood
Nottingham
Nottinghamshire
NG16 3BF

T: 0115 822 0200
E: info@your-itdepartment.co.uk
W: your-itdepartment.co.uk

Follow us on social media: