ACKNOWLEDGING
THE DARK WEB

(SURFACE) WEB

The level where data is PUBLIC
Only 4% of the web consists of indexed public websites that are visible to all web users through ordinary search engines such Google and Bing.

DEEP WEB

The level where data is PRIVATE
The largest part of the internet is made of protected information and is only located and accessed by a direct URL or IP address, that may require a password or other security access to get past public pages. That includes: email, online banking, social media pages & profiles, services such as video on demand, etc. It's used for legit purposes. Most of us access the Deep Web every day.

DARK WEB

The level where data is ANONYMOUS
Within the Deep Web is the part of the internet called the Dark Web. A complex encrypted system not visible to traditional search engines that can only be accessed by a special browser called Tor. Transactions, IPs, profiles, locations, etc. are totally anonymous, making it the perfect place for many illegal activities to happen. It's not illegal by itself but that's where criminal sites live.

IS IT ALL BAD? *NO. BUT IT'S QUITE BAD.*

There are several legit businesses operating on the Dark Web. Companies like Facebook and The New York Times are present on the Dark Web. It doesn't mean it's safe to do business there. The anonymity of the place attracts criminals trading illegal artifacts like guns, drugs and stolen data.

EVERYTHING HAS A PRICE

Dark Web businesses have the same structure as any legit e-commerce business does, including ratings & reviews, shopping carts, and forums. Kits for scamming and phishing are sold for as little as a $100 and stolen credentials to bank accounts can be found starting at $200 per account. The larger the available balance of an account, the higher its selling price. Credit card details are sold in bulk at reduced prices. Among the most valuable stolen credentials are keys that unlock privileged access to corporate networks, going for as much as $120,000.

HOW ALL THIS DATA ENDED UP HERE

The Verizon 2021 DBIR SMB study found that 85% of breaches involved the human element. Phishing was present in 36% of breaches. Furthermore, 61% of breaches involved credential data. 95% of organizations suffering credential-stuffing attacks had between 637 and 3.3 billion malicious login attempts through the year. The median for incidents with an impact was $21,659, with 95% of incidents falling between $826 and $653,587. The takeaway? Prevention is still the best plan.

WHAT YOUR DATA IS WORTH*

TV On Demand Credentials	*$10*
Scamming & Phishing Kits	*Starting at $100*
Bank Account Credentials	*Starting at $200*
Credit Card Information	*Bulk sales available*
Access to Corporate Network	*$120,000*

**Average prices based on recent Dark Web studies.*

61%
OF DATA BREACHES
INVOLVED CREDENTIAL DATA

IT WON'T HAPPEN TO YOUR BUSINESS. UNTIL IT HAPPENS.

Whether by user negligence or as a result of hacking, the chances of data exposure are high. The good news is that there are effective and affordable ways to prevent it. See some examples below.

CYBERSECURITY SOLUTIONS

Protect your business against internal and external threats with a comprehensive cybersecurity solution.

DARK WEB MONITORING

Get constant monitoring to ensure your company's data doesn't find its way to the Dark Web without you knowing.

SECURITY AWARENESS TRAINING

Teach your team how to ensure the links they click and websites they visit are authentic and not putting your business at risk.

CONTACT US TODAY TO FIND THE RIGHT SOLUTION FOR YOUR COMPANY

STAY CYBER SAFE!

OPTISTAR
TECHNOLOGY CONSULTANTS
A VERTEX COMPANY