GoodSuite
Speed • Innovation • Technology

What Is the Dark Web?

The Dark Web is only accessible via special browsers or software that allow the user to remain anonymous. Imagine the Dark Web to be like an unlit, hidden alley. You can't see the face of anyone when you peek inside; transactions are happening between people that aren't being seen, and individuals are moving freely, anonymously, and without a trace.

Nothing is tracked by search engines like Google or Bing, encryption hides identities, and to get into these secret areas, you need special software.

Like that dark alley, this is where dishonest behavior can thrive. If your information and identity are being exchanged on the Dark Web, you need to know so you can remedy things quickly.

Why is the Dark Web Dangerous?

If you don't want to be seen, then it's likely that you don't want to be caught. Cybercriminals buy and sell physical items like illegal drugs and guns, as well as electronic material like identities, passwords, hacking tools, and credit card numbers.

The problem is not only IF your credentials have been compromised, but WHAT you do next to protect yourself. Password reuse and lack of awareness of sophisticated phishing scams, like Business Email Compromise scams, means cybercriminals can use your own data against you.

Password Reuse

Once a password is found on the Dark Web, cybercriminals will attempt to use that password across any other accounts they can think of. If that password has been reused, particularly on a business account, not only is the employee at risk, but your organization is as well.

Business Email Compromise

Cybercriminals will use Dark Web data to create very targeted emails called Business Email Compromise (BEC) scams, where they impersonate key company executives to trick employees into carrying out their requests – often to transfer funds.

Internal Data Breach

Password reuse and Business Email Compromise scams are just two risks associated with having data on the Dark Web. This data can be used against you and your organization in several other ways, which may lead to an internal data breach for your organization.

What Is a Dark Web Scan?

By taking a dive into the depths of the Dark Web, we are able to perform a scan that searches for the presence of your organization's email domain. Cybercriminals on the Dark Web work hard to keep law enforcement and good-guy hackers from uncovering compromised data. So, while we do have human-verified data and a team hard at work cracking passwords, there may be more information on the Dark Web than what is being presented here today in this report. The Dark Web is large and complex, and there are locations that have yet to be penetrated and indexed. Therefore, it is imperative that you adopt a proactive approach of educating your users on possible phishing emails and other tactics that can result from breached dark web data.

This isn't a problem that is contained within borders – it's growing every single day, which is why you need to conduct ongoing monitoring of the Dark Web.

What Do the Results Mean?

We ran a Dark Web Scan of your domain and compiled all the results into this report. Our human operatives gathered all the data found, including passwords. Compromised data will vary depending on the type of data breach it was acquired from.

Compromised Data

The compromised data section shown on your report signifies what data has been found floating around on the Dark Web. The type of data can include name, address, email, etc. and can be used to craft sophisticated phishing scams.

Data Breach Details

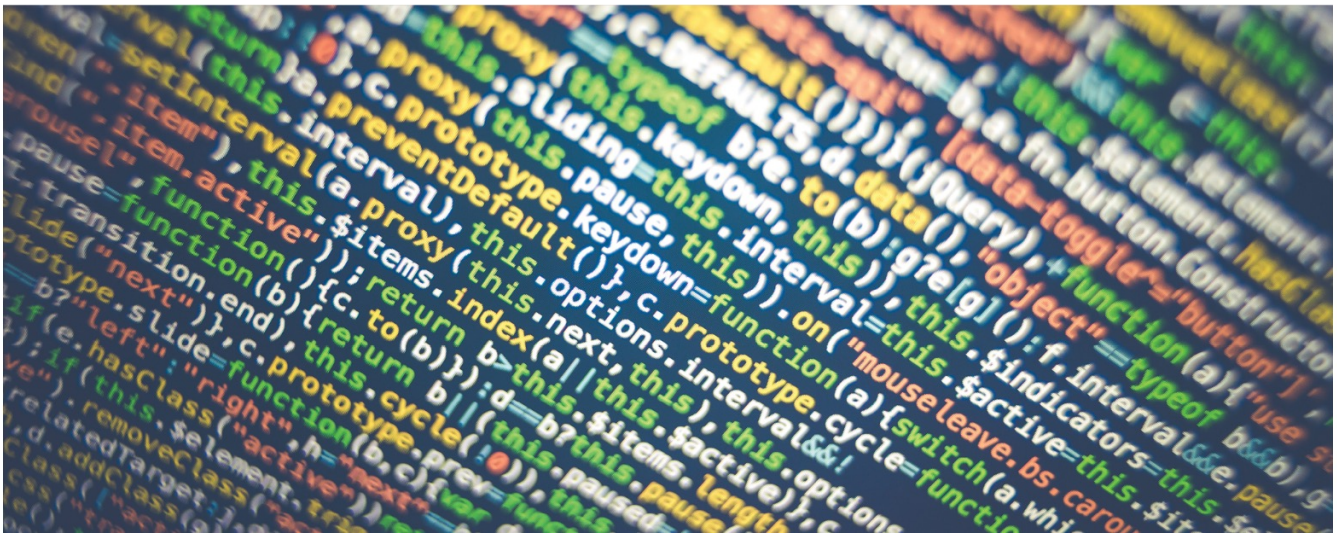
If there are known details of the data breach an employee has been involved in, they will appear in the Data Breach Details section of your report.

Breach Score

Each breach that your domain is found to be involved in will have a breach score associated with it. This score indicates how confident our research staff is that the data leak is from a credible source.

Passwords

If a password is found on the Dark Web, those details may be available. At times, passwords are compromised, however they have not yet been cracked – but that doesn't mean they are not at risk!



What Should I Do to Protect Myself and My Organization?

If your data was compromised - even one account, your credentials need to be attended to right away. The first thing you should do is change your passwords for any and all accounts you may have used that same password for. Passwords should be complex and a combination of at least 8-10 letters and characters. You should consider making your strong password a passphrase, which is a sequence of words meshed together. On an ongoing basis, you should always:

Use two-factor authentication

Two-factor authentication (2FA) is an extremely beneficial added security layer that requires users to provide extra proof that they are who they say they are when trying to log into their accounts.

Provide ongoing training & education

Cybersecurity threats are constantly changing and evolving. Ongoing training is necessary for your employees to stay up-to-date on current threats and best security practices.

Monitor your Dark Web status

New data breaches are discovered every hour of every day. A once and done Dark Web scan will not be enough to protect your Dark Web status ongoing. Continuous monitor equals constant protection.

Phish your employees regularly

In addition to training your employees on phishing, it is important that you put them to the test. Sending simulating phishing emails will help ensure employees know how to spot phishing attempts when they hit their inboxes.

Contact us today to learn how you can bundle in complete end-user security into your service. Dark Web Monitoring, Weekly Training, Ongoing Phishing, & more. Together we can strengthen the most targeted part of your network, your employees, into your most vigilant defense.