Dark Web Defender™
Frequently Asked Questions

DOCUMENT solutions
Business. Life. Simplified.

"What does this data mean?"

Typically, this data means that an employee used their work email as a user login on a third-party website, that website got breached, and the logins and passwords of that website are now compromised. So ultimately what is compromised is their work email along with a password.

My client already has two factor authentication; why do they need this service?

- Although most web services require two-factor authentication or 2FA, the strength and security vary.
- Easy for hackers to bypass weaker implementation by intercepting codes or exploiting account recovery systems.
- Most of the problems center around the fact that if you break through anything next to the 2FA login, (account-recovery process, trusted devices, or underlying carrier account) hackers are into the system anyway.
- The weakest point for 2FA is the wireless carrier (who can be breached) and the mobile device (which can be hacked).

"That is not my current password, I don't use it anymore."

This report provides historical as well as live real-time data. At one point in time, there was risk associated with these credentials and there could still be. 39% of adults in the U.S. are using the same or very similar passwords for multiple online sources. These passwords (whether active or not) are being used in phishing exercises and can be very compelling.

Ex: https://krebsonsecurity.com/2018/07/sextortion-scam-uses-recipients-hacked-passwords/

"That email is not someone who works at my organization."

An email address that is either not a valid email within the organization, or a "fake email" (ie: j12345@organization.com) may be a signal that the cyber handler/criminal is attempting a phishing attack on the organization. This is absolutely a reason for concern, as it makes it clear there has been active attempt at attack!

Email addresses discovered in the wild may not have ever existed on the Organization's mail server. Let's say that these email addresses were used to create accounts on some other service and it's that other service that is breached and the source of the Compromises. From our perspective, we can't determine if the email addresses we find in the wild are actual email addresses and therefore we report them.

Notes or comments regarding the credential or credential owner may also appear in our findings. For example, we've seen phone number and gender in the password field. While such a finding may not contain a password, the presence of the personal information in the record is still a valid finding.

"Why is there no password listed?"

We pull in very large data sets that include passwords. Sometimes in those data sets a variety of credentials do not include passwords, while in other cases, several categories of PII (Personally Identifiable Information) may have been exposed. (Ex. Name, DOB, Address, SSN)

Why does the PII matter in lieu of the password? Often, the categories of PII are extremely sensitive and may include credit card information or home addresses. These can be catastrophic to the individual, and it is an excellent opportunity for you (the MSP) to sell SpotLight ID as a secondary product offering.

"I just don't see the value of continuous monitoring."

"As your service provider, we believe Dark Web Defender acts like an early warning system by helping to mitigate the effects caused by a breach. We will be here to help you in case of any breach-related damage, but knowing about it early or preventing it altogether, is always a better launching point to ensure you are able to do what you do best"

"What is the difference between your service and Haveibeenpwned.com?"

Haveibeenpwned (HIBP) is a free service available to anyone. It is critical to understand these two main points:

- They DO NOT include passwords which makes it impossible to verify the data for your customers.
- The owner of HIBP Troy Hunt publicly admits via his blog:

> *"It should be abundantly clear from this post, but let me explicitly state it anyway: I have no idea how many of these are legitimate, how many are partially correct and how many are outright fabricated."*

“I’ve never used that password.”

In most cases when a password is coming up that an individual has never used, they have either forgotten they’ve used it before, someone is testing a password, or someone is creating a fictitious account for fraudulent purposes.

Often, when nefarious characters handle breach data, they work to put a value on the data. This may involve attempting to confirm the validity of a username/password combination. If such testing is positive, the password is often left in the source data. If the test is negative, the handler may fill in some placeholder value such as noted above to indicate that the username/password could not be confirmed as valid.

The DWD platform has controls in place which allow us to filter out password values that have been identified as “invalid;” you may notice some results from Live Search that have blank password fields. We do this to help avoid confusion.

You may be asking how much weight you should give a Compromise with a blank password or placeholder value. Our guidance is to treat such Compromises with the same weight you would one that has a clear text password. There may be a variety of reasons the handler chose to put in a placeholder value, but your clients’ credentials were found in a place known to be a source of nefarious activity and you should work to help them protect themselves from further exposure.

I showed the data and now the client is worried about additional exposure (as a result of the search).

The data we are pulling in is considered publicly available information. Our analysts DO NOT know who our Partners are, or who their clients are. They are pulling in credible credential exposures from the Dark Web, not placing it out there or using the data for any other purpose.

“The employee no longer works here, why should I care?”

This report includes lots of historical data, and you will see employees who no longer work at the organization. At the very least this should provide the opportunity to make sure all their permissions have been shut off. The real value of this data is the ongoing monitoring… you NEED to know about the credential exposure happening today, next week and next month. This also provides you as the MSP to speak about risk in general, to look at the behavior of past employees and current employees and speak to the need for other services like Security Training and Awareness programs and policy restrictions.

“I’m seeing multiple users with the same password being exposed on the same day, what does that mean?”

In most cases, someone is testing a password against a series of users to gain access.

I reached out to the IT Director, but no one wants to talk, and they are being defensive.

You must build the relationship with the internal IT Department and word your letters/emails to demonstrate you are there to partner with them, not to replace or unseat them. You can provide a service that they are not able to get on their own. Once you can ease their minds that you are not jeopardizing their job but simply want to provide enhanced security service and help them with the protection of the company, you will see them be more at ease. Tell them, “I am looking to work with you and help you with security monitoring for your company as you have xx credentials that are on the Dark Web, and we need to make sure people don’t get access to your network. We will work with you and you will have access to our portal, so your company is protected real-time on the Dark Web.”

“Why should I care if the password is encrypted?”

While initially a breach might include encrypted data, it’s important to understand that the data is only safe if the encryption key has not been published. Once the encryption key is published, much of that data is no longer safe. LinkedIn is a great example of this. 164M records were exposed in the LinkedIn breach. The passwords in the breach were stored as SHA1 hashes without salt, the majority of which were quickly cracked in the days following the release of the data.

“Under website it’s saying, “Not Disclosed,” … why should I care if it doesn’t say where it came from?”

While we do our best to provide as much attribution as possible, every category on the Dark Web is not always available and there are cases where we are waiting for public acknowledgment of a breach for legal purposes before assigning attribution to a specific website. With increased notification laws, we will see the speed of published attribution increase. We also retroactively provide attribution when we can.

It’s very important to shift your client or prospect’s attention away from “Not Disclosed” to the actual password, because if that is an active network password, variation of one or their banking password, then where it came from isn’t important. The fact that they need to do something is where the focus should be. If the password is something they are saying they’ve never used, a couple of things are in play, (1) They may not remember or they aren’t being honest (we’ve heard about this directly from Partners), or (2) Someone could be testing a password.