END-USER GUIDE

Dark Web ID

Understanding Your Dark Web Monitoring Protection

If you received a dark web alert, or want to understand how your organization monitors for credential theft, this guide explains what Dark Web ID does and what you need to do.

■ If you received an alert: Go directly to page 3 — Immediate Action Steps.

24B+	80%	207
credentials exposed on the dark web	breaches use stolen credentials	days avg to detect a breach without monitoring

Degarmo Technologies | degarmo.tech | July 2026

WHAT IS DARK WEB MONITORING

Your Credentials Are Being Watched — By Us

Dark Web ID monitors thousands of dark web sources to find your credentials before attackers can use them.

WHAT IS THE DARK WEB?

The dark web is a part of the internet not accessible through normal browsers. It requires special software to access and is home to illegal marketplaces where stolen data — including usernames and passwords — is bought and sold by cybercriminals.

HOW DID MY CREDENTIALS GET THERE?

Your credentials most likely appeared on the dark web because a third-party service you use was breached. When any website or application you've signed up for is hacked, the stolen credentials are harvested and eventually sold online. This is not your fault — it happens to organizations of all sizes worldwide.

WHAT DARK WEB ID DOES

Monitors Your Domains 24/7

Dark Web ID continuously scans over 600,000 websites, 500+ hacker IRC channels, and dark web forums — searching for any email address associated with your organization's domain.

Alerts Within Minutes

When your credentials are found, an alert is generated within minutes. Degarmo Technologies reviews the alert and contacts you with specific guidance on what to do next.

Searches Historical Data

Dark Web ID searches not just current listings but historical breach databases — giving you visibility into past exposures that may still pose risk if passwords haven't been changed.

Reports to Your Security Team

All findings are reported to your organization's security administrator and Degarmo Technologies, who coordinate the response and ensure the appropriate accounts are secured.

This Does Not Mean You Were Hacked

A dark web alert means your credentials were found in data stolen from a third party — not that your organization's systems were breached. It is a warning that gives you the opportunity to act before attackers do.

IMMEDIATE ACTION STEPS

You Received an Alert — Here Is What To Do Now

Follow these steps immediately. The faster you act, the lower your risk.

STEP-BY-STEP RESPONSE

Step 1: Don't Panic

An alert is an early warning — not confirmation of a breach. It means your credentials were found on the dark web, likely from a third-party site you used. You have time to respond effectively.

Step 2: Change the Exposed Password Immediately

Log in to the account associated with the exposed email address and change your password right now. Use a strong, unique password that you have not used anywhere else.

Step 3: Change It Everywhere You Reused That Password

If you used the same password on other sites (work email, banking, other accounts), change those passwords immediately as well. Credential stuffing attacks try stolen passwords across all major platforms.

Step 4: Enable Multi-Factor Authentication (MFA)

Turn on MFA for your work accounts and any other accounts that support it. Even if your password is stolen, MFA prevents attackers from logging in without access to your phone.

Step 5: Contact Your IT Team or Degarmo Technologies

Notify your IT administrator or contact Degarmo Technologies immediately. We will verify the alert, confirm which accounts are at risk, and guide you through any additional steps.

Step 6: Monitor for Suspicious Activity

Watch your work accounts, email, and any financial accounts associated with the exposed email for unusual activity over the next 30 days. Report anything unusual immediately.

Immediately Contact Degarmo Technologies

Call or email our team as soon as you receive an alert. We will help you assess the situation, prioritize your response, and ensure all exposed accounts are secured. Visit degarmo.tech for contact information.

STAYING PROTECTED

Password Best Practices After an Alert

Good password hygiene reduces your risk dramatically — and protects everyone around you.

WHAT MAKES A STRONG PASSWORD?

Length Over Complexity

A 16-character passphrase ("PurpleElephantJumped2024!") is far stronger than a short complex password ("P@s$w0rd"). Aim for at least 12-16 characters.

Unique Passwords Everywhere

Never reuse passwords across accounts. If one site is breached, a unique password means attackers cannot access your other accounts.

Use a Password Manager

Password managers (LastPass, 1Password, Bitwarden) store unique complex passwords for every site so you only need to remember one master password.

Enable MFA on Everything

Multi-factor authentication (a code sent to your phone or an authenticator app) is the single most effective control you can add after a strong password.

Never Share Passwords

Your password should never be shared — not with IT, not with colleagues, not with managers. If IT needs access, there are secure ways to provide it.

Change Periodically

Change your work account password at least every 90 days, or immediately if you suspect it may have been compromised.

You Are Part of Our Security Program

Your awareness and quick action after an alert is one of the most powerful security controls your organization has. Thank you for taking this seriously.

- **Same-day support from Degarmo Technologies**
- **Report all suspicious activity immediately**
- **No question is too small — ask us**

Visit degarmo.tech | Oklahoma City, OK | Veteran-Owned MSSP