HIGHTOWER

What to Do If Your Information Appears on the Dark Web

Learning that your personal information has appeared on the dark web can be unsettling. In many cases, however, it doesn't mean someone has accessed your financial accounts or stolen your identity. More often, it means information connected to you was exposed in a data breach and may now be circulating online.

The most important first step is understanding what information was exposed and deciding whether additional action is needed.

Step 1: Understand What Was Exposed

Not every data breach carries the same level of risk. The type of information involved often determines the appropriate response.

For example, an exposed email address may likely result in more phishing emails or spam. However, if a password were compromised, the password should be changed promptly, especially if it was reused across multiple accounts. If more sensitive information—such as your Social Security number or financial account credentials—was exposed, additional precautions may be warranted.

Before taking action, review any breach notification carefully to understand exactly what information was involved.

Step 2: Update Passwords and Strengthen Account Security

If passwords were exposed, change them as soon as possible, especially if you reused the same password across multiple accounts. Creating strong, complex passwords for important accounts can help limit the impact of future data breaches. Where available, enable multi-factor authentication (MFA) to add another layer of security and make it more difficult for unauthorized users to access your accounts. It's also a good idea to review your financial accounts for transactions or activity you don't recognize.

Step 3: Consider Additional Steps to Protect Your Identity

If sensitive personal information, such as your Social Security number or date of birth, was exposed, you may want to place a credit freeze with the major credit bureaus. A credit freeze makes it more difficult for someone to open a new account in your name without your authorization, while still allowing you to temporarily lift the freeze if you need to apply for credit. You should also review your credit reports periodically for accounts or inquiries you don't recognize.

Step 4: Be Cautious of Follow-Up Scams

Cybercriminals often take advantage of high-profile data breaches by sending phishing emails, text messages and phone calls that appear more credible because they reference the incident.

These messages may ask you to verify account information, reset a password or confirm recent activity. Before responding, verify that the communication came from the organization it claims to represent. Whenever possible, contact the organization using a phone number or website you already know rather than information provided in an unsolicited message.

Step 5: Know What Monitoring Services Can and Can't Do

Identity theft protection and dark web monitoring services can notify you when information connected to you appears in places associated with cybercrime. While these services can provide valuable awareness, they cannot remove your personal information from the internet or prevent fraud from occurring.

Instead, monitoring services are most effective when used as one part of a broader approach to protecting your digital identity.

remember these steps

If you find that your information has appeared on the dark web, remember these action steps:

- Confirm the notification came from a legitimate source
- Determine what information was exposed
- Update any affected passwords and avoid reusing passwords across accounts
- Enable multi-factor authentication where available
- Consider placing a security freeze if sensitive personal information was exposed
- Review your financial accounts and credit reports for unfamiliar activity.
- Remain alert for phishing emails, phone calls and text messages related to the breach

If you have questions about protecting your financial accounts after a data breach or receive a suspicious request involving your finances, reach out to your financial advisor. They can help you think through the situation and connect you with the appropriate resources before you take action.

HIGHTOWER

200 W MADISON, 25TH FLOOR
CHICAGO, IL 60606

(312) 962-3800
HIGHTOWERADVISORS.COM