Norton LifeLock

Dark Web Guide

Dark Web notifications inform you that your information has been exposed and available to cybercriminals. We monitor for use of your personal information on these hard to find dark websites and forums and notify you when we detect it.

Cybercriminals can use your information to hack into accounts and commit fraudulent activities. Here we have included different steps you can take to help protect your personal information, along with additional information on what is the Dark Web.

What is the dark web and how does it differ from the deep and surface web?

The surface web comprises of websites that are indexed (or catalogued) by search engines. The dark web is a hidden layer of the internet that is not accessible or indexed by search engines and requires specific software for access. This area is popular with criminals because they can remain anonymous and untraceable as they communicate. The dark web is a huge marketplace where hackers and thieves exchange information, goods and services; information exposed from data breaches, hacking incidents, or leaked information can be bought and sold on the dark web as “lists” by identity thieves. Information traded on the dark web may be old or could even re-appear several months, or years following exposure of your personal information. The dark web forms a small part of the deep web.

What is a Dark Web Monitoring Notification?

Dark Web Monitoring, also known as cyber monitoring, is a service that helps monitor for information on the dark web and notifies you if we detect your information on the dark web. The notification that you receive is called a Dark Web Monitoring Notification.

How does one access the dark web?

The dark web is accessible only if you download a special open-source browser software . Such software typically uses encryption technology to help users maintain their anonymity online. It does this, in part, by routing connections through servers around the world, making them much harder to track.

Dark Web Guide

I have never been on the dark web. How did my information get on the dark web?

You do not need to be on the dark web for your information to end up there. Information stolen or exposed in data breaches or hacking incidents, or leaked information can be bought and sold on the dark web as “lists” by identity thieves. This information may be old or could even re-appear several months, or years following exposure of the information.

Can you erase my information from the dark web?

We do not erase information from the dark web because of the highly anonymous nature of forums, communities, and black markets in which criminals operate.

What is a Baseline Notification?

When you enroll, we run a one-time historical dark web scan looking back to 2008 to determine if the information you provided us has been previously exposed. If we find exposed information, we notify you. This is known as a Historical or Baseline Notification.

What role does Norton Dark Web Monitoring Powered by LifeLock play in helping to protect my information?

As part of your service, we scan the surface, deep, and dark web for exposure of information. When you enroll, we run a one-time historical dark web scan looking back to 2008 to determine if the information you provided us has been previously exposed. If we find exposed information, we notify you. We run continuous scans and are on the lookout for exposed information. If your information has been exposed, you can be proactive and take several actions to help protect yourself. You can:

- ✓ **Change the password associated** with the affected website or any other site where you’ve used the same password. If you don’t remember your password, perform a password reset on the site.
- ✓ **Review your credit reports**, and watch for new credit inquiry alerts, or suspicious activity, and consider freezing your credit file
- ✓ If you have signed up for Transaction Monitoring, **review your financial transactions regularly**
- ✓ **Complete your profile** by visiting the dashboard so we can monitor more of your information
- ✓ **Visit our Dark Web Monitoring Support Article** for a full list of other helpful tips and guidance.

Why am I getting notification from a breach that happened several months ago?

The dark web is where stolen information, such as bank account numbers, and credit card numbers, are sold. The information sold or traded can be in the form of “lists” which can be old, and could even re-appear several months, or years following an exposure of the information. Every time the information reappears or resurfaces on the dark web, you are likely to be notified.

“Exposed” information does not necessarily mean that your account(s) have been hacked. Given that these lists may be old, it is entirely possible that your login details associated with the website/service in question are no longer current. You may have already changed a password, deactivated your account or unsubscribed from the website or service. Sometimes breached sites deactivate exposed accounts, as well, which may make it difficult to remember or identify an account as belonging to you.

What does it mean to have my information exposed on the dark web? Have my accounts been hacked?

“Exposed” information does not necessarily mean that your account(s) have been hacked. You can be proactive and take several actions to help protect yourself. Change your password for the site/service mentioned in the notification. In addition, if you use the same password for numerous online accounts, make sure you change these passwords as well. Enable two-factor authentication whenever offered by a site or service. Visit our Dark Web Monitoring Support Article for a full list of helpful tips and guidance.

Why can’t I respond to the Dark Web Monitoring Notification to confirm my identity?

For some alerts, we ask you for a confirmation of the activity or transaction so we can determine if there might have been the possibility of an identity theft incident.
For other notifications, such as Dark Web Monitoring, we are notifying you that information which may belong to you has been detected. These notifications do not require confirmation from you because it is a result of a scan we perform on your behalf, and not a result of your activity.
When you receive a Dark Web Monitoring Notification, follow the helpful tips and guidance in the Dark Web Monitoring Support Article to help protect yourself.
You do not need to call us.

What actions can I take to help protect myself?

You can be proactive and take several actions to help protect yourself. Change your password for the site/service mentioned in the notification. In addition, if you use the same password for numerous online accounts, make sure you change these passwords as well. Enable two-factor authentication whenever offered by a site. Monitor your credit report for any unfamiliar or suspicious activity. Visit our Dark Web Monitoring Support Article for a full list of helpful tips and guidance.

I don’t recognize the website mentioned in my Dark Web Monitoring Notification. How do I know I have used this before?

There could be several reasons why you may not recognize the website mentioned in a notification. For example, the account may have been created via Facebook or Google log in. Some accounts may be old and you may not remember having used the website or service. In some instances, you may have provided login details (username/password) for a one-time use, after which you may have never went back to the website or account again. Sometimes breached sites or services may deactivate exposed accounts which can make it difficult to remember or identify an account as belonging to you.

Can my personal information be exposed if I have unsubscribed from a website or deactivated my account?

Even though you may have unsubscribed from a website or may have deactivated your account, your data may still be present in their data systems and could be exposed during a data breach, a hacking incident, or another type of data leak.

What is the difference between the Exposed Information and the Additional Exposed Information sections within the Dark Web Monitoring Notification?

Your Dark Web Monitoring Notification displays two types of exposed information. When you enroll you provide us information and we monitor it actively. If we detect this information on the Dark Web, it will be displayed in the Exposed Information section of the Dark Web Monitoring Notification. If we detect other exposed information that may be related to you, we will notify you on this as well.

Even if you did not provide the specific information to us, it is possible to use the information you have provided to help detect other information that may have been exposed; but since we have not collected this information from you, we can only notify you that it has been exposed, and not provide any other details. For example, in the case of a healthcare database breach, if you have provided your Insurance Account and Insurance Provider information for monitoring, we may also be able to notify you of additional data that may have been exposed, such as blood type, prescription medications, diagnoses, and related details. This type of information would be displayed in the Additional Exposed Information section of the Dark Web Monitoring Notification.

Dark Web Guide

Next Steps

to take if you have been made aware of other information being breached

Username/Password

□ Change your username if you have the option.

□ Change your passwords linked to that username.

□ Set up 2-factor authentication whenever available for a website. You can visit https://twofactorauth.org/ for more information.

Email Address

□ Change your email account password.

□ Set up 2-factor authentication whenever available for a website. You can visit https://twofactorauth.org/ for more information.

□ If you are using this email as a login/username for websites, consider changing the username and passwords to those websites for better protection.

Social Security Number

□ Check your credit report regularly for unauthorized activity.

□ Put a credit freeze on your credit file.

□ Put a security freeze on your consumer report with the National Consumer Telecom & Utilities Exchange and ChexSystems.

□ Register for an online account with the Social Security Administration to securely access information from your Social Security record, including earnings and benefits history.

Bank Account

□ Monitor your account activity closely. Report any suspicious activity, such as unfamiliar purchases, to your financial institution immediately.

□ Contact your bank for a replacement account.

□ Change your online banking username if you have the option

□ Change your online banking password.
Set up 2-factor authentication if available.
You can visit https://twofactorauth.org/ for more information.

□ We recommend using LifeLock's Transaction Monitoring feature, available in the Member Portal with some LifeLock identity theft protection memberships.

Credit/Debit Card

□ Request a replacement card and new PIN.

□ Monitor your account activity closely. Report any suspicious activity to your financial institution immediately.

□ Change your online account username if you have the option.

□ Change your online account password.

□ Set up 2-factor authentication if available.
You can visit https://twofactorauth.org/ for more information.

□ We recommend using LifeLock's Transaction Monitoring feature, available in the Member Portal with some LifeLock identity theft protection memberships.

More Helpful Tips

□ If you use the same Username and Passwords for multiple websites or apps, change them when there is a breach

□ Think before you download apps, click on links, or reply to emails that might be harmful or fraudulent.

□ Be suspicious of strangers who ask for personal information by email. If they claim to be from your financial institution, the government or a company you do business with, contact the business directly.

□ Don't use all or part of your Social Security number as a PIN (Personal Identification Number) for a credit/debit card or an online account username or password.