IDShield™

Five Steps to Take in the Event of a Cyberattack

Has your email account ever been hacked? If you answered "yes", then you have been the victim of a cyberattack. In today's world, these hack attempts are becoming increasingly common. Frequent data breaches and other cyberattacks we hear about in the news, serve as a reminder for us all to be vigilant and take extra precautions to ensure our privacy is protected.

The steps below can help you better protect yourself from cyberattacks.

1 Update your passwords

Better security starts with better passwords. In the event of a rise in hack attempts, it is safe to update all passwords. You can use a password manager to generate and store your passwords. A different password should be created for each account. Examples of the most popular passwords found on the dark web that should NOT be used include, Abc123, 111111, Iloveyou and Password.

2 Do not use public wi-fi

Be mindful if you need to use public wi-fi. It is always better to connect to a VPN, especially when handling financial transactions.

3 Update security settings on social media accounts

Check security settings on your social media accounts. It is safer if your account is marked as private or if content is only accessible to friends. It's also best to ignore friend requests from people you do not know.

4 Be skeptical about links and attachments

Be wary of emails and text messages with URLs. If you're not sure about the source, don't use the link or open the attachment. This rule should also be followed when using social media messaging platforms.

5 Review money sharing apps

It is a good idea to link your credit cards and not debit cards on your money sharing apps and to make sure you have set up two- factor authentication. You can also turn on alerts, to proactively monitor your account's activity.

You can take control of your security by being proactive. An identity theft protection plan like IDShield can help you protect your privacy by monitoring your usernames and passwords across the dark web. We can also monitor your financial accounts for unauthorized transactions.

If you are enrolled in IDShield and think you are a victim of a cyberattack such as having your email account hacked, please call to speak to an IDShield identity theft specialist. If you are not enrolled in IDShield, you can enroll during your employer's next open enrollment period.

US_BU_NP_ID_IN_EN_CyberattacksGuide_85x11_v1_053122