

Your Online Financial Profile Got Hacked — Now What?

What to do when you realize that your identity has been compromised

Few things can bring on a sense of panic and confusion quicker than realizing that your financial information is compromised. Whether you find yourself unable to access your financial institution's online app because the password has changed, notice fraudulent charges made to your credit card, or are suddenly missing money from your checking or savings account, the feeling that your financial security is at risk is a terrifying one. The best reaction to such a situation is a measured one that follows certain steps to recovery.

Notify your financial institution

Whether the account in question is a savings or checking account or a credit card, your immediate action in response to hacking should be to contact your financial institution. The FTC recommends following up initial communications with an email or letter that confirms your account information, the time and date when you first noticed the fraudulent activity, and when you first contacted your financial institution.

The quicker you notify the financial institution, the quicker you can shut down additional transactions or withdrawals, so it's important to act in a timely fashion. According to the FTC, you will not be held financially liable for any unauthorized transactions made using your debit card number when the card is not lost if you report those transactions within 60 days.

PC Magazine Lead Analyst Neil Rubenking writes that credit card fraud is even easier than when someone has gained access to a savings or checking account. Companies will investigate and will not hold you responsible if the charges in question are found to be fraudulent. Once you're issued a new card, the problem is ostensibly solved.

Update your security

If your online login or password has been compromised, the FTC recommends immediately changing your password and, if possible, your username. If you're locked out of your account because someone else has access, contact your financial institution and they'll help protect your account and recover it. When you craft your new username and password, you'll want to make sure that it is unique — don't share a password with any other accounts you have and avoid overly simplistic passwords.

Once your online account has been restored, take additional steps to secure it so that you won't have to worry about a reoccurrence. Marc Saltzman, writing for AARP, recommends enabling two-factor authentication like using your thumbprint for an app or receiving a one-time access code via mobile phone whenever you log in. Saltzman also recommends making sure that your security software is up to date so that you are better protected from viruses and malware.

Dig deeper into your credit report

The fact that someone has gained access to a financial account of yours might indicate a larger problem with your identity, particularly if it shared a common password with other accounts. Not only should you do a full sweep of your sensitive information to check for suspicious activity and update security settings, but the FTC strongly recommends checking your credit report.

You are entitled to a free report from each of the three major credit reporting agencies every 12 months by visiting [AnnualCreditReport.com](https://www.annualcreditreport.com). Use these reports to make sure that there are no lines of credit open that you did not open yourself and that your payment history is accurate. Knowing this information is crucial not just when you have your identity compromised, but also if you plan to

take out a loan in the future. You may also want to consider opting into a credit monitoring service, which Saltzman notes are often available through your credit card company or financial institution.

Dealing with being hacked is an unpleasant experience in any respect, but if you know how to approach the situation, you'll be better prepared to protect yourself and move on from the incident unscathed.