What to Do When You've Been Hacked

By Neil J. Rubenking, PCMag.com, Updated February 15, 2022

When your email, credit card, or identity gets hacked, it can be a nightmare. Knowing what to expect can be a help; knowing how to head off the hackers is even better. Our guide helps with both.

In the modern online world, privacy is a rare commodity. Big corporations know all about you, aided by data brokers that collect and collate all the data crumbs you leave as you wander the internet. But this lack of privacy is nothing compared to what happens if a criminal hacking team digs deep into your personal information. Big companies want to sell you stuff; hacker crews want to steal your stuff. They'll monetize their unauthorized access to your life as quickly and thoroughly as they can, preferably before you even know there's a problem. Some experts prognosticate that 2022 will be the biggest year ever for data breaches. Sooner or later, your personal life will be exposed. What can you do when you realize that you've been hacked?

How Will You Know?

When a major hack attack or data breach occurs, it's all over the news. Frequently the affected service spins up a web page where you can check whether you were affected. And you will be affected, if not this time then the next. The only upside is that you're one among possibly millions, so the hackers may never get around to weaponizing your details. Don't imagine that you can prevent a breach. The antivirus running on your computer is utterly powerless against a security attack on a faraway server.

Not every hack starts with a well-publicized data breach. Your credit card could be compromised by a shady online merchant, a card skimmer, or even a waiter in a brick-and-mortar restaurant. The first clue may be the appearance of unexpected items on the credit card bill. Always read those bills and figure out what every line means, even the small charges. Card thieves will occasionally put through a few small purchases, just to make sure the card is "live," before making a big purchase. You can use a personal finance service, such as Mint, to keep an eye on all your credit card transactions from one place.

Banks are good at fraud detection these days. There's a good chance you won't learn about a compromised card until after the bank declines the charges and starts the process for issuing a new card. Getting a new card is a pain, as any automatic payments you've configured will need the new card number. Still, it's better than letting hackers buy an 85-inch TV with your credit.

Credit card numbers aren't the only kind of data that hackers can misuse. Scammers can use a compromised email account to broadcast spam or to send targeted email scams to your contacts. Your first clue may be worried phone calls from friends asking if you're truly stuck in a Dubai airport with no cash, or irate messages from those "you" have spammed.

An identity thief can also use your personal information to open credit accounts, accounts you know nothing about. You might only find out about those accounts when a merchant slams the door on your request to open a new line of credit yourself. Cagey consumers use AnnualCreditReport.com to request a free report from Equifax, Experian, and TransUnion once per year, spreading the requests out at four-month intervals. Yes, Equifax experienced a major breach and had to pay $650 million in damages for its negligence, including free credit monitoring or a $125 minimum payout for anyone affected. But you were affected regardless of whether you checked credit with Equifax.

PCMag thinks highly of the Credit Karma service, which automatically pulls your credit from TransUnion and Equifax every week to keep an eye on your credit. These are "soft" inquiries, not the "hard" inquiries that companies make when you apply for more credit. Hard inquiries can erode your credit score; soft inquiries have no effect.

A change in your credit score is like a ripple in a pond, where the actual misuse of your credit is the rock that made the ripple. Services like Avast BreachGuard and IDX Privacy aim their sights at those rocks. They regularly monitor the Dark Web to make sure your personal data hasn't come up for sale. Norton 360 Deluxe includes a similar scan, powered in part by the company's LifeLock identity theft remediation technology.

Breach monitoring is also a bonus in some password manager tools, notably Keeper and LastPass. The connection makes sense because the first thing to do when a site gets breached is to change your password for that site. With the password manager's help, you can change it to a strong, unique password that you don't use for any other site.

What Happens Next?

Credit card compromise may be the easiest hack to get over. You're not responsible for the fraudulent charges, and once the bank has issued a new card the problem is solved. Well, except for the need to update your payment information anywhere the old card was saved.

Regaining control of a hacked email account can be tougher. You'll have to contact the email provider and prove that you're the true account holder. Of course, if the hacker changes your password, you can't use your regular email to contact the provider. It's important to have more than one email address and make each the alternate contact address for the other.

Many websites force you to use your email address as the username for your account. That's certainly easier than making you choose (and remember) a unique username and a unique password for every site. But if you used the password from your hacked email account at any other sites, those accounts are now popularized too. A hacker who gets hold of your login credentials for one site will invariably try the same username and password pair on dozens of other popular sites.

Even if you don't use any duplicate passwords, compromise of your email account can still be a huge problem. Think about this. If you forget a website password, what do you do? Right—you click to get a password reset link sent to your email address. A smart hacker who has control of the email account will quickly seek your other accounts, social media, perhaps, or worse, shopping and banking accounts. After a simple password reset, the hacker owns those accounts too. After recovering from an email account takeover, you absolutely should visit every site that's associated with that email address and change your password. A password manager will be a great help here.

Get Help for Identity Theft

Full-on identity theft can be a nightmare. Victims can spend thousands of dollars over weeks and months trying to get their online identities and lives back in their control. The Federal Trade Commission offers an excellent advice site (https://www.consumer.ftc.gov/features/feature-0014-identity-theft) with full details on how you can proceed. Among other things, the site suggests that you order your credit reports, so you can see what's happened, and make an official identity theft report with the FTC.

The site goes on to specify absolutely everything you need to do in step-by-step fashion. It includes checklists so you can make sure you didn't miss any tasks, as well as sample letters and forms. You won't go wrong relying on this useful resource.

You've seen the ads for third-party identity theft remediation services. These can help, but only if you have their protection in place before something drastic happens. It's not unlike an insurance policy—you pay for the protection, but hope you'll never have to use it. Adding such a service to your monthly bills won't clean up the breach you just suffered, but it should help the next time around.