Responding to a breach...

These steps will help you to make positive changes to protect yourself.

1. Change your passwords: Start with the service that was breached and the things you use most. Think banking, email, online shopping, social media.

2. Turn on 2FA ('two-factor authentication'): This makes it harder for someone to get into your account by asking for two codes or 'factors' before unlocking. Even if someone has your password, they don't have the second 'factor' - often a code sent to your phone. The Authy website lets you search for platforms that have 2FA and walks you through the setup.

3. Notify your bank and freeze your credit score, if needed: Depending on the breach, you may want to contact your bank and credit bureau. (Or whichever organisation holds credit scores in your country.) This stops people applying for new credit cards in your name, and so stops the problem spreading. Local consumer advocacy groups can also help. Your bank will talk through whether you need new account numbers and cards.

4. Tell your 'trust circle' what's happened: This is your close group of friends and relatives. It puts them on the lookout for any unusual phone calls or emails from potential scammers.

Now you can look at to what do to contain the damage of the actual breach.

5. See what you can find online: You may want to check for whether or not your personal information is out there. What information can you find whilst casually looking? Start with your normal search engine and search terms that aren't revealing on their own i.e. search your name and the last 4 digits of your phone number, but not your whole phone number. Firefox Monitor lets you search for whether your information has been breached and you can sign up there for the latest breach news.

6. Petition websites directly to remove your data: Let's say you've got a job interview coming up and aren't happy with what search results show about you. You can contact a website directly to remove your data, according to your rights as set out in the General Data Protection Regulation (GDPR). A lot of websites are keen to comply with the new data protection laws brought in by GDPR so if you ask them to take down information, they'll often do so quickly to avoid hassle and cost. Generally speaking, if the product or service is offered within the EU, then the data processing needs to comply with the GDPR, whether or not the company or you are physically located there.

You can also use services that will get your data deleted for you. Websites such as Reputation Defender, Privacy Duck, and Abine's 'Delete Me' will contact websites to delete your information. They charge fees but also have more information on how you can do it yourself too.

TACTICAL TECH

DATA DETOX KIT

#datadetox
datadetoxkit.org

Updated: January 2021

Steps that you can take anytime...

1. Look at what data you have online: (Start with important accounts like email, banking, shopping and chat)
Ask yourself:

1. Where do I have accounts with data on me?
2. How could this be problematic if breached?
3. Why is it there? (does it need to be?)
   What is their security like? Go into the website's privacy and terms of service and look for terms like: 'encrypted at rest' or 'encrypted in transit' that mean your data is stored securely.
4. What is their access policy and length of storage?
   Does it say in the terms of service if all staff can access your information? What's their data retention policy? If a website doesn't mention how long they keep your data for- the answer is probably forever.

2. Regularly de-clutter and reduce: If services don't have your data, it can't leak or breach. If they only have information from the last 3 months, that's all that can be breached. So take a regular approach to de-cluttering your online data. Ask yourself: 'why would I keep this?.' Delete what you don't need and download anything you do, so that you can remove the data from the website or app.

3. Check again: Can you strengthen my protections? (better passwords and 2FA) Do your security and system updates.

4. Tell companies to take better care of your data: Some people say that there will always be breaches, just like there will always be crime. But companies can also do more to protect your data. Contacting them can get their attention that they need to listen and act. For example, send a tweet that says 'we want to know how long you keep our data, it should be not forever.