Checklist: When you're notified that your data has been leaked

Intended purpose:

The intended purpose of this checklist is to be referred to when you find out your data has been breached. This checklist is also designed to be used **in conjunction with** any guidance provided by the affected company, **not in place of it**. Note that depending on the breach not all of these items may be applicable.

Typically, you will receive an email from an affected business informing you that their systems have been compromised and your data was involved. However, it's not strictly limited to instances involving your relationship to a business, you can utilise a lot of this advice when any of your accounts are suspected to have been breach. **Don't wait for a notification if there are signs** because smaller businesses or less reputable ones won't send out a timely notification to affected customers.

You may have been linked here from our related article linked here which prompted the creation of this checklist. The example in the article involved bad actors demanding a ransom from the affected company before the data was eventually released on the Dark Web weeks later. In similar examples time can be somewhat on your side (even though the bad actors did analyse the data) meaning you can be more methodical rather than reckless.

However, if it's not part of such a large-scale breach involving negotiations for ransom **you will need to act much quicker**. We say this to give the 'Immediately' heading below context based on the situation.

TIP: It's a good idea to **keep a handwritten record of what you're doing** as you may be flustered and it's unlikely you will complete each step start to finish in one sitting. Simply list the accounts you've changed your passwords with, so you know which ones you need to come back to. Keep a record of the time and name of any operator you speak to when contacting organisations and similar notes.

Immediately:

- [ ] First **confirm that the notification is real!** Bad actors may send out phishing emails claiming your data has been compromised in an attempt to have you panic click on any (malicious) links they include in the notification. If you read our related article you'll recall it included a timeline of announcements from the affected company as an example. This included **television and online news coverage** as well as **posting confirmation and updates on their website** – this is a sure sign of the legitimacy of the breach. **Call the company or visit the website manually** – don't go through links if there isn't any mass media coverage.

THINK: For the next steps the name of the game **is reducing future risk by invalidating the data which was breached**. The breached data is out there in the hands of the bad actors, there is nothing you can do to undo that. So, **your mindset needs to move to devaluing and invalidating** as much of it as you're able to change. **Passwords and numbers** are key, numbers include both account numbers and identity / identity document numbers.

- [ ] Starting with passwords, **change all of your passwords <u>in priority order</u>**, don't take false comfort when companies say passwords are encrypted. Bad actors have tools with algorithms which can crack weak passwords at the simpler end of the spectrum. Consider activating 2FA while you're logged in and changing settings.

1. The priority is **any username / email address and password, or similar password used with the online account of the breached company** is most at risk. Bad actors will use these to try access other commonly linked accounts.
2. Next, change the passwords to **high value accounts** such as **email** accounts which can be used for password resets as well as **banking, cloud storage, social media**, and anywhere with such significance.
3. Finally, change the passwords to any accounts that don't fit the previous two categories. This will just be accounts that you rarely use and which don't hold significant data about you.

Now think about the leaked **numbers** and consider:

- [ ] Contact your bank if your financial information has been breached, inform them, put a freeze on your accounts, and request new cards. **Ensure you have some access to funds in some way before instigating this** due to the lag in receiving new cards.

- [ ] Visit your transport department and request a new Driver's Licence if yours was breached.

- [ ] Contact the relevant department in your country if your passport or other state issued identity document was breached

- [ ] If any medical or healthcare information was stolen contact your health insurer and/or relevant healthcare department and notify them. Depending on the healthcare system in your country and what you pay for in addition to that (such as your own private health insurance) request new card / identification numbers.

- [ ] Consider changing your mobile number and **remember to update all 2FA before your outgoing number is deactivated**

The goal is that the leaked password and leaked number/s will be rejected or declined if they attempt to be used. The password will be wrong and not give account access, the credit card number will be wrong and decline attempted transactions, the identity or healthcare number will be invalid and not process claims, etc.

From here reflect on any other risks that may exist for you as we're moving to territory with more individual or specific risks.

- Consider alerting your professional relationships and alert them to be vigilant of any suspicious activity posing as you. Think business partners, business clients, employers and colleagues, regular doctor, family or business lawyer, etc.
- Did the breach involve any information relating to your spouse or children? Should they perform some of these actions?
- Can the breach have any impact on your reputation or employment status, particularly if you rely on a public image?

In the weeks to follow:

Understand this is the time you will be at most risk of some kind of scam or fraud as a result of the data breach. Be on high alert and extra vigilant of phishing scams or suspicious messaging through any medium. Monitor your bank account statements, sent box in your email accounts, relevant types of history (purchase, login, etc) within accounts.

Unfortunately, as a worst-case scenario **you may need to go a bit cold with online communications and your mindset should be 'distrust at first unless verified'** meaning:

- Don't click on any links sent by email, SMS, social media or any online medium. Visit sites by manually typing the address, make phone calls by manually typing numbers, etc
- Instigate the opening of new accounts yourself, do not complete any online application forms linked to you
- Do not give remote access to your device/s unless you've explicitly verified it is your trusted IT support
- Verify the account numbers of any invoices you need to pay, contact the company's Accounts department by phone and verify their back account details are the same as what's on the invoice.

Some final longer-term or ongoing actions to consider are:

☐ Obtain a credit report to **ensure no accounts or loans have been opened in your name**. These are free for the first report in most countries, and usually free on a prescribed basis ongoing (e.g., one every three months) with more regular requests usually attracting a small fee.

☐ Consider signing up for **credit monitoring or identity protection services**. Many of these have additional benefits such as Dark Web monitoring to notify you if your data is found to be on sale there, for example.

☐ Contact your doctor's office and request your medical history to see if someone has posed as you in a healthcare visit

Links:

Our articles and guides on related topics:

[Phishing 101]
[Two Factor Authentication (2FA)]
[Setting Strong Passwords]
[Identity Theft 101]
[What to do when identity theft strikes]
[The Dark Web]
[What bad actors want]