Two Factor Authentication (2FA)

Dray Agha / 06 May 2020

2FA is **an essential security** layer to make hackers' lives much more difficult. Passwords are a basic form of authentication but as we know they are not perfect.

2FA is the answer to our password woes.

How It Works

A website will ask for a 2FA code to **authenticate** your identity. Authentication, confirming you are who you say you are, is based on a number of premises. Most relevant to our discussion are:

- something you **know** (for example a password or your mothers' maiden name)
- something you **have** (for example a mobile phone, or a bank card)

2FA combines something you KNOW with something you HAVE. A hacker with your password **does not** immediately have details like your mothers' maiden name, nor does the hacker have your mobile phone. So, they will be unable to answer the 2FA question after they try and login with your password.

How You Use it

You can set 2FA up by logging into the web service as usual and then going into the **settings** where it will usually say "*Turn on Two-Factor Authentication*". Once on, it will protect your account in the future by asking for a specific number that it will send to you after you have put your password in. It may send you this number via:

- A text
- An email
- An authenticator app.
- A USB 'key' is growing in popularity but isn't the most affordable option yet.

For now**, authenticator apps are the best ways to go about 2FA.** They produce one-time **rolling number codes**, with a countdown. Once the countdown has lapsed, a new one-time code is produced and the previous one becomes unusable.

Not Perfect

There are **still** ways for hackers to attack your account, even if you activate 2FA:

- Hackers could phone up and trick you into giving the code. A web service will never ask for your code, so you will know you're on a scam phone call **if your 2FA details are requested.**
- Though rare, **hackers have been able to trick mobile phone companies** into sending over a new version of your sim card to them, and they then use your sim card to receive 2FA codes. If this is a concern for you, **stick to using an authenticator app.**

Most websites do not ask for 2FA by default, and you instead have to turn it on yourself. This isn't ideal, and some companies are learning to ask for 2FA by default **after they suffer a security breach.**

Authentication apps are secure but can **become frustrating**. Some of the apps do not store your details online, so **if your phone is lost or stolen,** and you download the authenticator app on a new phone, the codes will not be loaded on there. Which is a huge inconvenience. There are some authentication apps who **do** store your details in their cloud storage, so read up on the different authentication providers and find one that works for you.

2FA Considerations with Employees

Security can become complicated if you want **employees** to have 2FA**. A former employee** holding a device with your 2FA keys has the potential to do a lot of damage to your online resources. To manage this security risk:

- Part of **the departure process** for an exiting employee should always be a housekeeping of their IT credentials, which includes **removing their 2FA tokens** from their **device**.
- There are **dedicated 2FA providers** who can offer administrative management for the 2FA accounts of your employees.

Backup Codes

The mismanagement of **backup codes** is a security risk that **isn't spoken about enough** on the topic of 2FA.

When first setting up 2FA, the webservice will offer you backup codes- a list of one-time pass codes that are a safety net in case you lose access to your original method of 2FA. **These backup codes are able to override whatever settings** you had on your phone for 2FA, and log you in to your account.

You may have the option to download your backup codes or screenshot them. **It is a huge security issue** if you do this and then leave **a digital copy** sitting in your Downloads folder! **Hackers *will* find a way to access this list of master codes if you leave them lying around.**

It is better to store these backup codes **offline.** Print them, put them somewhere safe and don't be tempted to save them online.

Convenience V Inconvenience

For the sake of convenience, most web services ask for your 2FA once and then allow you to stay logged in for a set amount of time (an hour, a week, a month etc). This is a reasonable trade-off of security versus convenience, so you don't have to re-input your 2FA codes every time you navigate to the page.

If there's a particular service integral to your workflow that doesn't support 2FA, or offer a similar authentication security layer, it is perhaps worth switching to a service that does offer these settings. **2FA cannot be underestimated**. It really is a massive obstacle to the average Hacker.

Further guidance:

- https://www.ncsc.gov.uk/guidance/setting-two-factor-authentication-2fa
- https://www.ncsc.gov.uk/guidance/multi-factor-authentication-online-services

Dray Agha is a PhD Researcher based in the Information Security Department at Royal Holloway University of London