Chris’ talk - Q & A

Anonymous Attendee 12:55 PM

Who is behind "have I been pwned"? Do we know it is safe to use it?

Reply:

This is really about context: basically HIBP is trying to provide a safe way to check if someone already knows your password. And that is inherently unsafe to begin with.

To understand a bit more about how websites handle passwords, I can recommend reading https://www.theguardian.com/technology/2016/dec/15/passwords-hacking-hashing-salting-sha-2 (or search for “passwords and hacking explained the guardian” in your favourite search engine).

At its core, HIBP technically uses publicly available information: it’s a database of “fingerprints” of passwords (called hashes) which have been found somewhere on the internet associated with a particular email address. Rather than simply making that data more accessible, HIBP takes additional steps to improve the security of the data it finds, respecting the principle of responsible disclosure.

Perhaps the only contentious feature is the ability to check if a particular password has been seen before, which could inadvertently share data that isn’t already in the public domain (for instance, checking a password that hasn’t yet been stolen). But there are alternative ways to do this, for example HIBP provides an API you can use to search for a hash you create yourself, which a number of password managers already use to check if a password been used before – without disclosing your actual password.

Which means that HIBP is probably the safest way for most people to check whether their password is on the dark web somewhere.

Anonymous Attendee 12:55 PM

wouldn't it be very easy to filter out these sub adresses?

Reply:

In theory yes. However I don’t think there’s much to gain by doing it: leaving the list un-filtered is quick, easy, and delivers a message to everyone’s inbox; filtering may not require that much effort, but could reduce the number of inboxes a hacker hits. The real question is whether a spammer actually cares if their target knows where they got the data from?

The clear exceptions here are targeted attacks like spear phishing and whaling: these are tailored messages that might even be hand-crafted in order to look as legitimate and real as possible.

Anonymous Attendee 12:55 PM

It is also great if you can use your own domain and have an email provider that supports a "catch all" functionality and then you can generate random (based on a hash) email address and give one to each website. :-)

Reply:

For certain specific cases, a simpler option may be to use a disposable email address instead. These generally allow you to create a random email address to use for a specific period of time (from 10 minutes up to 24hrs), letting you sign up and receive content – such as a download link, or activation code – without ever having to share your actual email. When the time expires, the account is deleted.

But, these shouldn't be used if you have to share real personal data! Although the accounts are randomly generated, there's a chance someone could get the same address in future. If you gave any personal data when you registered with that email, it may be shared with someone else while they have access to the mailbox. You'll also have no way to unsubscribe or un-register once the account has timed out.

For one-time or throw-away registrations where you can provide bogus/fake data (like getting an activation code for a WiFi hotspot, or a download link for some software, or documentation) disposable emails can be a handy way to avoid spam.

Anonymous Attendee 12:56 PM

How Save and reliable is the haveibeenpwned Page re. Data privacy ;-)

Reply: See answer above.

Anonymous Attendee 12:58 PM

how the password manager configured over the many devices that we might use to access services (phone, tablets, professionnal computer, personal computer, etc...) ?

Reply:

Most password managers use a cloud service to synchronise the data between your different devices. In principle, this means that a "master copy" of your data is stored safely somewhere on the internet, so that every app you log in to on any device can take a copy. Changes made on that device are then copied back to the cloud, ensuring all versions are up to date.

There are some apps that allow you to create a file on your home network as the "master copy", rather than in the cloud. Your apps will copy any changes to it whenever you re-connect to your home WiFi. The main challenge with these types of setups is ensuring that your file is protected against someone copying it from your network.

Check out https://restoreprivacy.com/password-manager/ (or search for "restore privacy password manager" in your favourite search engine) for a great overview of the different features available in the latest password managers, and some independent reviews for many of the products available.

Anonymous Attendee 12:58 PM

Which is your preferred password manager?

Reply:

I've used a number of different ones in the past, for different use cases and situations. Currently I use a combination of KeyPass, KeyPassXC, and 1Password.

Different managers offer different features that may be more attractive to different people. Check out https://restoreprivacy.com/password-manager/ (or search for "restore privacy password manager" in your favourite search engine) to understand what features are available, and decide which tools might suit you best: try one out and see how it goes.

Antoine Duparay 12:58 PM

if you don't use a password manager (yet), tip of the day: choose a strong password (qwe8a!AD for example), and then concate the first and the last 2 letters of the domain name you are registering, at the beginning and at the end: if you register at cern.ch, you take ce + pwd + rn and your password would be ceqwe8a!ADrn. Bam, unique password everywhere, with only one password to remember ;)

Reply:

Thank you for this – it is better than having the same password everywhere, but there is scope for a poor pattern/structure to give a false sense of security. Using dictionary words and known/disclosed passwords can reduce the amount of effort an attacker needs to guess your password.

If you rely on passwords alone, then complexity and length are essential, but this makes it inherently difficult to for us to naturally remember. Until we find a real alternative to passwords, two-factor authentication and a password manager are the safest approach.

Anonymous Attendee 12:59 PM

Are online password managers really safe?

Reply:

If you use a strong password, and enable two factor authentication, then a suitably protected password manager account can offer far greater safety for your passwords, than many people could achieve without one. There are a lot of guides online explaining the best ways to do this for each specific service – it's definitely worth searching these out when setting up an account.

It's important to re-iterate that different services offer different features, which can affect the perception of how safe they are.

For example, 1Password encrypts your data in a way that if you forget your account password, you're locked out: even 1Password can't recover it for you. Whereas LastPass offers an "emergency access" mode that allows you to share your passwords with other users (such as family members). Some may find this kind of feature incredibly useful for peace of mind, others may think the same for 1Password's approach.

Check out https://restoreprivacy.com/password-manager/ (or search for "restore privacy password manager" in your favourite search engine) to learn a bit more about the features these tools provide, and for some independent reviews of the services currently available.

Anonymous Attendee 01:00 PM

While I appreciate the discussions about what each of us can do to improve our own privacy, perhaps a better use of one's energy is to make the more difficult step to stop using services that exploit personal data for profit. As long as we fuel this commercial exploitation by providing our personal data, nothing will change.

And, perhaps we should spend more energy advocating that our own organisations also stop their support for commercial exploitation of personal data. This means no facebook/twitter/instagram/youtube/gsuite/etc. for our organisations. Otherwise, we just keep feeding this privacy exploiting beast.

Curious about your opinions on this more consequential approach?

Reply:

For official services, we do have obligations to ensure the use of these services are in line with applicable policy and process, which will include compliance requirements for protection of personal data. These obligations will limit the scope with which many types of services may be used in an official capacity – especially the "free" consumer variants. However, the terms and conditions available to paying customers – or even, that can be negotiated between companies where a specific mutual interest exists – do usually offer the type of measures organisations need in order to meet their compliance requirements.

One of the biggest challenges for organisations such as ours right now, is the fact that these services – in particular the free ones – are so accessible: as a user, you no longer have to wait for the IT department to set something up for you (or for finance to buy something); you can just sign up yourself. Raising awareness of the complexities involved their use – for these presentations, the personal impact of the data they handle – are a way to help stem the flow of data to them through their unofficial use.

If there is a sufficiently strong motivation for an organisation to use these types of services, then surely the best use of our time is in ensuring it can use them responsibly?

Liviu Valsan

E-mail sub-adressing (RFC 5233) still links the email aaddress to your primary email identity. Whatever comes after the "+" sign can be easily removed in order to obtain your primary email address. Having true email aliasing, allowing to create an infinite number of aliases that have absolutely no connection to your primary email identity is much more privacy preserving. But of course, many email providers (especially the "free" ones where the business model is to monetize the data of their users) do not offer such a functionality.

Reply:

You're quite right. There is no guarantee that this doesn't happen; we can simply hypothesise about how likely it may be.

Similarly, true addressing is a great approach for those technically able to set it up and maintain it. The difficulty is making it easy enough for everyone to use.

Vincent Brillault 01:00 PM

What do you think of password managers built-in web browsers? In particular the Firefox one

Reply:

Lockerwise – the one built into Firefox – has a number of features that offer reasonable protection (such as requiring you to repeat your computer password to view/copy passwords, and notifications that warn you if a password has been seen on the internet somewhere), but I wouldn't say it's at the same level as the dedicated manager apps, which is to be expected.

Dedicated apps are designed purely for that purpose, based upon extensive, focused user feedback. All the work they do is spent making the tool more secure and more functional. Built-in tools like lockerwise are just one feature within the bigger browser project; while there may be effort to improve how they work, it simply wouldn't get the same level of attention as a dedicated app.

Generally speaking, built-in managers are a legacy of the built-in features designed for convenience, that are now being retro-fitted with security add-ons. Dedicated password apps have been developed with security in mind from the start, wrapped up in convenience features designed to remove the hassle.

Anonymous Attendee 01:02 PM

Troy Hunt is the person behind the have i been pwned? service. You can see here (https://haveibeenpwned.com/Privacy) how the service works and how it handles data. We actually had the opportunity to have him give a talk at CERN. He has a good reputation and all the info about the service is available on his blog/service page. He is quite a public person, who was also invited to give a testimony to the US Congress https://www.troyhunt.com/heres-what-im-telling-us-congress-about-data-breaches/

Reply: Thank you for mentioning this and highlighting the information.

clambole 01:04 PM

Is there a danger to reply ok remember me for the last time and ok to save the pw for the next login to secured platforms?

Reply:

There's a number of ways these functionalities can work, but I'll focus on what seems to be the most likely.

Many browsers allow you to save login details inside their built-in password managers. Very old browsers don't really protect this information, so the general recommendation is to avoid it. Modern ones can offer some protection, but it varies between browser. The general danger is that the data could be easily seen by someone else who has access to your computer.

If the check box is built into a web page (such as at the bottom of a log-in form), then it's probably a feature of the web page itself to set a cookie on your computer to save the username for you. Cookies are small text files that websites can create to store small pieces of information. Whenever you visit the page, it can look up which cookies it created and use them to provide persistence between visits: like auto-filling your username, or remembering what language you chose, or a particular style/theme you like etc without you having to log in. These types of cookies generally don't present any real danger.

If you want to save passwords to make life easier, the safest option would be to use a dedicated password manager.

Anonymous Attendee 01:16 PM

Isn't using online password managers or that synchronize online a security risk? At the end of the day you need to trust on the provider. Isn't it better to keep everything local and potentially synchronize via a secure channel? I have personally used the combination KeepPassXC+Nextcloud as a great solution.

Reply:

This is really a question about relative risk and opportunity. If you have the skills and knowledge to set up and operate what is in effect a private cloud, then it's an opportunity you're uniquely able to exploit that may reduce certain risks but increase others in relation to a public-cloud alternative.

But that opportunity isn't universal, and for the vast majority of people, an online password manager provides a convenient way to massively reduce the risk they're exposed to, when compared with their current approaches.

And that's really the point here: online services provide the most accessible way for most people to safely manage their online identities.