Master Password

Your sites are in danger: a primer on passwords

Your passwords are… terrible

Passwords are the doors to our virtual homes. They are all that stand between the people of the world and your personal property, your privacy, your valued possessions, your reputation and your identity.

And despite these immensely high stakes, the fact that our passwords are in fact *terrible*, is a very badly kept secret – if not already public knowledge.

Passwords are the elephant in the room when we talk about how precious the things we keep in our online accounts are to us. We all know how pressing, dangerous and ominous this problem of ours is. But despite our best efforts, we just can't seem to get it right. Or worse – we tell ourselves we did.

What is going on?

Every so often, usually when another high profile person has had their accounts hacked, we are reminded of how we should be doing passwords in order to keep safe. Don't use simple words, names; mix in letters, symbols, make them cryptic, use completely different cryptic words for every site. We read these tips and nod in agreement, then move on with our lives and leave this as a problem to solve on another other day.

The truth is, it's not our fault. So, what is really going on here?
Password protection is everywhere. Not because it's good for you, but because it's easy for them. Every account you own on the net, everything of yours that others shouldn't get into, every bit of your data on a company's servers, needs to be protected. And *the password* just happens to be a cheap and universally understood solution that allows companies to yield the responsibility of access control to **you**.

Never mind that you are merely human and don't have the cognitive capacity to handle this task for every account you own on the web.

Password managers are not the answer

I know what you're thinking. You've heard this story before. And the solution, you've tried it too. Or maybe you still are – trying.

Password managers are pieces of software created to be the light in the dark – the answer to the problem. Finally a place to save all of these complex passwords of yours, available whenever you need them. They may even make randomly complex passwords for you. What a relief. But is it really?

The grievances of trying to introduce a password manager into our life are many, but if you've tried, you may recognize at least several of these:

- Your office, home and mobile app need to sync.
  If they don't or a problem occurs, you find yourself unable to access accounts you made from another device.
- You need to make good *backups*, and keep them constantly up-to-date.
  Usually, the time you discover you messed this up is also the time something else has already gone horribly wrong.
- You need to *trust* a company with keys to *all* of your doors.
  Even scarier than losing all of your passwords is reading in the news that somebody hacked your password manager's company servers and copied them.
- You *depend* on your device to get into your accounts.
  Finally your laptop is all set up. But now you're at a client, on a trip or at a friend's. Your accounts do not belong to you – they belong to your password manager.

What went wrong?

Password managers were a good and brave first attempt at solving a very difficult problem. They were a solution inspired by our first reflex: when drowning in complexity, we reach for paper and offload the task of remembering all of these cryptic passwords and codes onto a notepad. Password managers are simply the virtual equivalent, but they are just as much a band-aid solution as the original reflex was.

We need to go back to what passwords are supposed to be, and stop violating the principle that underpins why they work: passwords belong in our heads, nowhere else.

Your password, your identity

You have accounts everywhere. And every week you make one somewhere new. But all of these accounts share a very important commonality: they are all yours. Together, they make up your online identity.

Sometimes, in a wishful moment, we would just use a single password for all of them. Our password. Because they are all ours. But then we remember that we're smarter than that. We don't really want to give eBay our email password, or the company our Facebook password. But we wish we could. Because what we really want is to look at our accounts as our virtual home and our password as our front door keys.

Your master password

You're ready.

Master Password is an algorithm developed by Maarten Billemont, designed to unlock all your doors with one set of keys, but leave them securely shut for anyone else.

At the very core of Master Password is the principle that each of your accounts must be sealed by highly secure, unique and unguessable locks, keeping each account independently isolated, while giving you a single password, trivial to remember, to unlock them all.

In simple terms, your virtual life is a rented building and only you hold the master key.