

Perfect Computer Security Is a Myth. But It's Still Important

By **Justin Pot** on February 14th, 2018

Maybe you've heard it before: "Security is a myth." It's become a common refrain after a never-ending string of high-profile security breaches. If Fortune 500 companies with million dollar security budgets can't lock things down, how can you?

And there's truth to this: *perfect* security is a myth. No matter what you do, no matter how careful you are, you will never be 100 percent safe from hackers, malware, and cybercrime. That's the reality we all live in, and it's important to keep this in mind, if only so that we can all feel more sympathy for victims.

But remember: perfect is the enemy of good. *Perfect* security is a myth, but that doesn't mean [resolving to lock down your tech](#) is pointless. You'll never be completely safe, but that's no reason to stop caring about security all together.

Locking Your Front Door Is Pointless

The lock on your front door is useless. A decent locksmith can get in easily, with a pick or with a drill. If that doesn't work, someone could just throw a brick through your window. If a burglar wants to get into your house, they will.

Is that depressing? Yes. Does it mean you shouldn't bother to lock your door? Absolutely not.

Locking your door won't stop everyone from getting into your house, but it does make it just a little harder to get in. This keeps teenagers out if nothing else, and means that professionals need to deal with your door while neighbours are potentially watching. Locking your door doesn't totally prevent theft, but that doesn't mean it does nothing.

Cyber security is the same way. Using the same password for every site is the online equivalent of leaving your door unlocked, because [a breach on one site reveals your password for every other one](#). It's why every tech blog you read [keeps talking about password managers like LastPass](#).

Every security tip is like this. Things like [two factor authentication](#) aren't perfect, but they're far, far better than passwords alone. Every software update will probably still

have bugs and potential exploits, but that's no reason to avoid patching the ones that are documented now.

In other words: yes, someone might smash your window. Lock your door anyway.

Think About Your Threat Level

I'll admit something awful here: I re-use passwords from time to time. Am I stupid? Possibly, but mostly there are just some sites I don't care about. If someone wants to access my Super Burger Place Rewards account, they can go for it, but they won't find a credit card or any personal information attached when they get in. Enjoy being four tenths of the way to a free burger, I guess?

What I absolutely lock down are my email, social, and banking accounts, along with any online services that store my credit card information. I know I could potentially lose a lot of money, and I know that personal information about me could become public. I'd rather avoid that if I could, so those accounts all have different usernames, passwords, and two factor authentication enabled.

I know this isn't foolproof. I know that, if someone with enough experience really wants to get in, they probably could. But if a site has information worth protecting I try to protect it, because doing something is better than doing nothing.

It's All About Balance

Personal security isn't about doing everything you can to prevent hacking, because doing absolutely everything is a full time job. Personal security is about finding a balance between possible threats and things you can do to alleviate them. Your username and password will probably be revealed during a breach, so you shouldn't use the same one everywhere. Your computer can be stolen pretty easily, so you should [encrypt the hard drive](#)—because almost everything on there is sensitive, and it's [shockingly easy to get past a login password](#). Think through potential threats, then find ways to alleviate them.

Only you can work out what's best for your needs, but I implore you not to throw up your hands and give up completely. Perfect security may not be possible, but that doesn't mean you shouldn't even try.