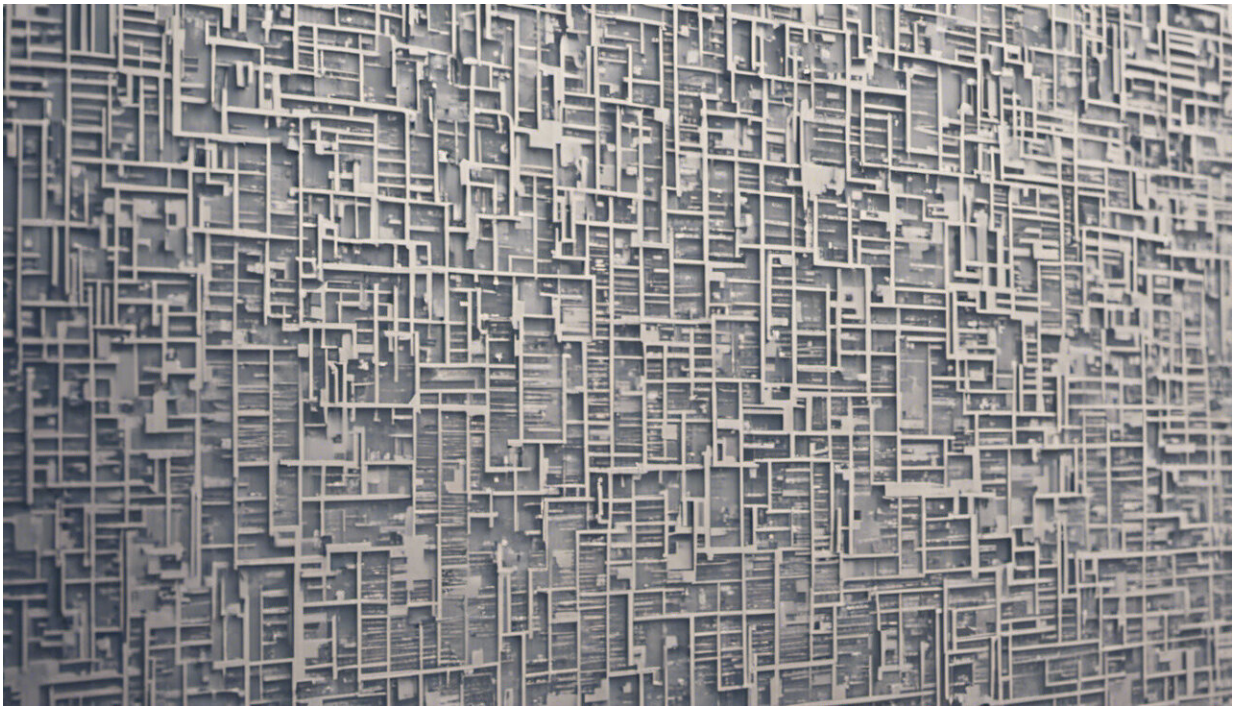
Data breaches are inevitable – here's how to protect yourself anyway

January 18 2019, by W. David Salisbury And Rusty Baldwin



Credit: AI-generated image (disclaimer)

It's tempting to give up on data security altogether, with all the billions of pieces of personal data – Social Security numbers, credit cards, home addresses, phone numbers, passwords and much more – breached and stolen in recent years. But that's not realistic – nor is the idea of going offline entirely. In any case, huge data-collection corporations vacuum

up data about almost every American without their knowledge.

As cybersecurity researchers, we offer good news to brighten this bleak picture. There are some simple ways to protect your personal data that can still be effective, though they involve changing how you think about your own information security.

The main thing is to assume that you are a target. Though most individual people aren't specifically being watched, software that mines massive troves of data – enhanced by artificial intelligence – can target vast numbers of people almost as easily as any one person. Think defensively about how you can protect yourself from an almost inevitable attack, rather than assuming you'll avoid harm.

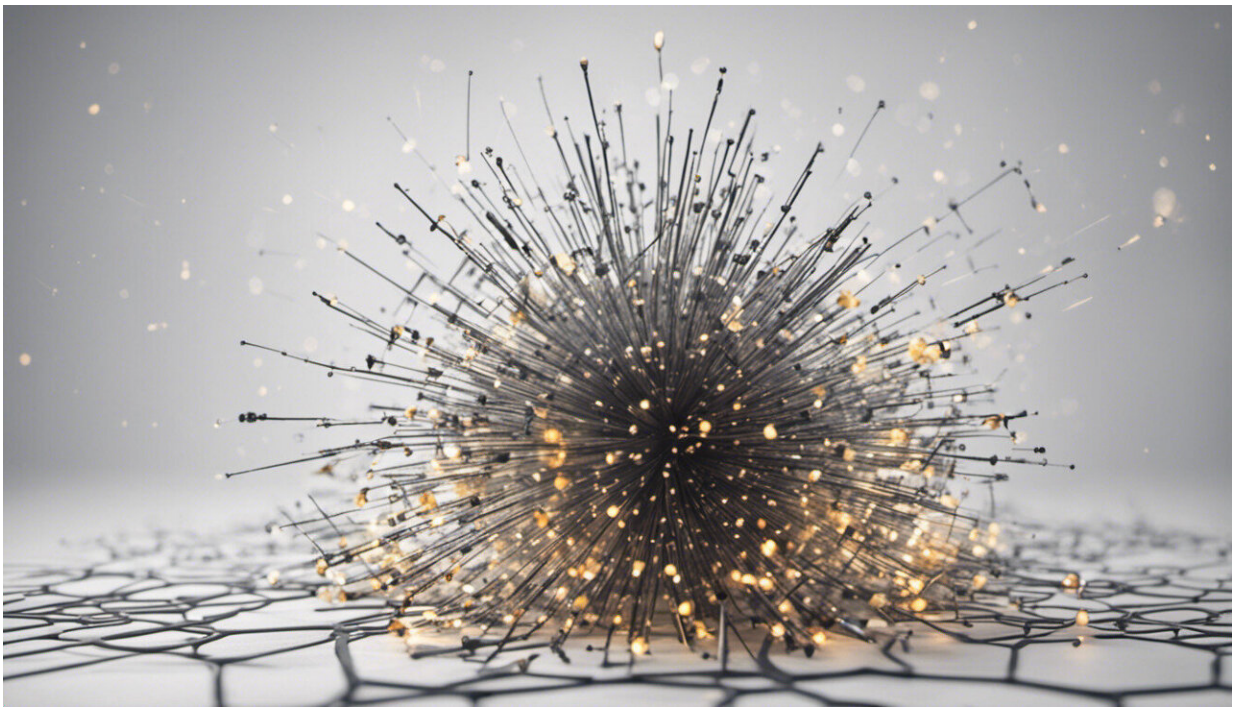
What's most important now?

That said, it's unproductive and frustrating to think you must pay attention to every possible avenue of attack. Simplify your approach by focusing on what information you most want to protect.

Covering the obvious, keep your software up-to-date. Software companies issue updates when they fix security vulnerabilities, but if you don't download and install them, you're leaving yourself unprotected from malware such as keystroke loggers. Also, be smart about what links you click in your email or when browsing the web – you could inadvertently download malicious software to your phone or computer, or allow hackers access to your online accounts.

In terms of online data, the most important information to protect is your login credentials for key accounts – like banking, government services, email and social media. You can't do much about how well websites and companies safeguard your information, but you can make it harder for hackers to get into your account, or at least more than one of them.

How? The first step is to use a different username and password on each crucial site or service. This can be complicated by sites' limits on username options – or their dependence on email addresses. Similarly, many sites have requirements on passwords that limit their length or the number or type of characters that they can include. But do your best.



Credit: AI-generated image (disclaimer)

The reason for this is straightforward: When a bunch of usernames and passwords fall into malicious hands, hackers know it's human nature to repeat usernames and passwords across many sites. So they almost immediately start trying those combinations anywhere they can – like major banks and email services. A chief information security officer we know in the banking industry told us that after the Yahoo breach of a few years ago, banking sites were hit with multiple attempts to log in

with credentials stolen from Yahoo.

Use long passwords

There has been a lot of research about what makes a strong password – which has often led to many people using complex passwords like "7hi5!sMyP@s4w0rd." But more recent research suggests that what matters much more is that passwords are long. That's what makes them more resistant to an attempt to guess them by trying many different options. Longer passwords don't have to be harder to remember: They could be easily recalled phrases like "MyFirstCarWasAToyotaCorolla" or "InHighSchoolIWon9Cross-CountryRaces."

It can be daunting to think about remembering all these different usernames and passwords. Password management software can help – though choose carefully as more than one of them have been breached. It can be even safer – despite conventional wisdom and decades of security advice – to write them down, so long as you trust everyone who has access to your home.

Use a third line of defense

To add another layer of protection – including against troublesome housemates – many sites (Google, for example) let you turn on what's called multi-factor authentication. This can be an app on your smartphone that generates a numeric code every 30 seconds or so, or a physical item you plug into your computer's USB port. While they can afford at least some protection, be wary of sites that send you a text with a code; that method is vulnerable to interception.

With these straightforward steps – and the new mindset of thinking like a target who wants to avoid getting hit – you'll be far less worried when

news breaks of the next breach of some company's enormous data files. Bad guys may get one of your usernames, and maybe even one of your passwords – so you'll have to change those. But they won't have all your credentials for all your online accounts. And if you use multi-factor authentication, the bad guys might not even be able to get into the account whose credentials they just stole.

Focus on what's most important to protect, and use simple – but effective – methods to protect yourself and your information.

Provided by The Conversation