# How vulnerable is your personal information? Four essential reads

**Eric Smalley, *The Conversation***

When you enter your personal information or credit card number into a website, do you have a moment of hesitation? A nagging sense of vulnerability prompted by the parade of headlines about data breaches and hacks? If so, you probably push those feelings aside and hit the submit button, because, well, you need to shop, apply for that job, file that insurance claim, apply for that loan, or do any of the other sensitive activities that take place online these days.

First, the bad news. If you regularly enter sensitive information online, chances are you've had some data stolen somewhere at some point. By one estimate, the average American had data stolen at least four times in 2019. And the hits keep coming. For instance, a data breach at the wireless carrier T-Mobile reported in August 2021 affected 100 million people.

Now for some good news. Not all hacks are the same, and there are steps you can take to protect yourself. The Conversation gathered four articles from our archives that illuminate the types of threats to your online data, what data thieves do with your stolen information, and what you can do about it.

## 1. Take stock of your risk

Not all cyberattacks are the same, and not all personal data is the same. Was an organization that has your information the victim of a ransomware attack? Chances are your information won't be stolen, though the organization's copy of it could be rendered unusable.

If an organization you deal with did have customer data stolen, what data of yours did the thieves get? Merrill Warkentin, a professor of information systems at Mississippi State University, writes that you should ask yourself some questions to assess your risk. If the stolen data was your purchase history, maybe that won't be used to hurt you. But if it was your credit card number, that's a different story.

Data breaches are a good opportunity "to change your passwords, especially at banks, brokerages and any site that retains your credit card number," he wrote. In addition to using unique passwords and two-factor authentication, "you should also consider closing old unused accounts so that the information associated with them is no longer available."

## 2. The market for your stolen data

Most data breaches are financial crimes, but the hackers generally don't use the stolen data themselves. Instead, they sell it on the black market, usually via websites on the dark web, for other criminals and scammers to use.

This black market is awash in personal data, so much so that your information is probably worth a lot less than you would guess. For example, stolen PayPal account information goes for $30.

Buyers use stolen data in several ways, writes Ravi Sen, an associate professor of information and operations management at Texas A&M University. Common uses are stealing your money or identity. "Credit card numbers and security codes can be used to create clone cards for making fraudulent transactions," he writes. "Social Security numbers, home addresses, full names, dates of birth and other personally identifiable information can be used in identity theft."

## 3. How to prepare for the inevitable

With all this bad news, it's tempting to throw up your hands and assume there's nothing you can do. W. David Salisbury, a professor of cybersecurity management, and Rusty Baldwin, a research professor of computer science at the University of Dayton, write that there are steps you can take to protect yourself.

[*Over 140,000 readers rely on The Conversation's newsletters to understand the world.* Sign up today.]

"Think defensively about how you can protect yourself from an almost inevitable attack, rather than assuming you'll avoid harm," they write. The key is focusing on the information that's most important to protect. Uppermost are your passwords, particularly for banking and government services. Use different passwords for different sites, and use long – though not necessarily complicated – passwords, they write.

The most effective way to protect your data is to add another layer of security via multifactor authentication. And rather than rely on websites to text or email you authentication codes, which can be hijacked, you should use an app or USB device that uses public-key encryption, they write.

## 4. Don't make it easy for the thieves

The risk to your personal information isn't just having it stolen from a third party. Phishing attacks can get you to do the thieves' work for them. These emails fool people into entering personal information and passwords on fake websites controlled by data thieves.

It turns out that you're probably pretty good at sensing when something is off about an email message. Rick Wash, an associate professor of information science and cybersecurity at Michigan State University, found that the average person is as good as a cybersecurity expert at sensing when something is weird about an email message.

The trick to protecting yourself from phishing attacks is remembering that phishing exists and could explain what you're sensing about an email message.

"The people who were good at noticing phishing messages reported stories about specific phishing incidents they had heard about," he wrote. "Familiarity with specific phishing incidents helps people remember phishing generally."

*Editor's note: This story is a roundup of articles from The Conversation's archives.*

Eric Smalley, Science + Technology Editor, *The Conversation*