I Should Worry. But I Don't.

Most of us refuse to protect ourselves against hackers. Why is that?

BY PUNAM A. KELLER

I HAVE A CONFESSION. Despite alarming odds of being hacked, I use the same password to access my computer desktop, iTunes account, PayPal, and an embarrassingly large number of online-shopping sites.

It gets worse. I have not changed this password in three years, and I consistently ignore software update reminders.

It's not that I'm uninformed about the risks. Rarely a day goes by that I don't see a report about full-time hackers plundering credit cards, stealing identities and draining bank accounts.

When I read such news, however, my first reaction is to deny the threat is real.

I have the same cavalier disregard for danger in other matters. I do not pay attention to news stories about the fragility of our Social Security system, discoveries of terrorist activity in my state, or warnings of escalating health-care costs.

Economists call this rational inattention. The idea is that individuals have a limited amount of attention and therefore must choose which information to attend to carefully, which information to attend to less carefully, and which information to ignore.

As if this weren't bad enough, let me also bring up something that psychologists call "protection motivation theory." This theory says that the main reasons people don't act in the face of a likely threat are that they don't believe (1) that they are vulnerable, (2) that the threat is severe, or (3) that any action will really keep them safe.

So, the question becomes, can I—and apparently lots of people like me—overcome both rational inattention and the protection motivation theory to be made to believe that hacking threats are a real danger to us, and that there are things we can do to protect ourselves?

I believe the answer is yes. And as a marketing professor and a behavior-change expert, I have come up with five recommendations for ways to increase protection motivation.

GETTY IMAGES

The first reaction to yet another hacking headline is often denial.

Some People Never Learn

Every year, SplashData, a maker of password-management applications, publishes a list of the worst passwords—those that appear most often in files containing stolen passwords posted online by hackers. And every year, many of the same easy-to-remember and easy-to-hack passwords appear on the list, a strong indication that people's bad password habits are very hard to break. Here are the 20 worst passwords from the latest list:

1 123456	6 123456789	11 1234567	16 mustang
2 password	7 1234	12 monkey	17 access
3 12345	8 baseball	13 letmein	18 shadow
4 12345678	9 dragon	14 abc123	19 master
5 qwerty	10 football	15 111111	20 michael

Source: SplashData Inc.

THE WALL STREET JOURNAL.

1. MAKE THE THREAT MORE PERSONAL.

Instead of simply asking people to add anti-spyware programs, ask people questions that make the threat hit home. Ask, for example, if they want to know when someone may be spying on them. Last year, after consumer accounts at major retailers like Target and Home Depot were breached, I declared myself invulnerable because I don't shop at either of those stores. I would have paid more attention if I was prompted to consider the possibility of my favorite retail outlet being the next target.

2. MAKE THE PROTECTION MORE RELEVANT AND EASIER TO UNDERSTAND.

It is more difficult to deny threats when you can see yourself being attacked or find out that you cannot depend on safety in numbers.

For example, when I read the news that a Russian crime ring had stolen 1.2 billion username and password combinations, I figured I was pretty safe since there are seven billion people on Earth. I would be more motivated to protect myself if I was told the Russian crime ring was targeting American women. Similarly, I would be more motivated to upgrade my software if the accompanying message from the software company explained how I am receiving greater protection instead of just telling me I am getting more sophisticated stuff.

3. CUT THE NUMBER OF STEPS.

The less we have to do to gain security, the more likely we are to do it. For example, systems could be designed so that computers don't have to be plugged in to receive software downloads; companies also could reduce the need for users to act by making antivirus software the default. If some types of auto-upgrades are impossible, people can be nudged to protect themselves by being asked to choose between two options: I want the new software because I want to protect the information on my computer, or I do not want the new software even if the information on my computer is less protected.

4. PROVIDE AN EFFECTIVE SOLUTION.

When a practical solution is offered, we are more likely to change our behavior. The use of digital fingerprints is easy and foolproof: A fingerprint is hard to copy and never changes. Or let someone (or something) else, like a password manager, generate passwords and save users' credentials for each website. My research shows that people are willing to acknowledge they are at risk if they believe there is something they can do to protect themselves. For example, there are smokers who are not willing to do something about quitting smoking—which entails believing that they are at risk of getting lung cancer—until they are shown how easy it is to use a nicotine patch.

5. OVERCOME COGNITIVE BARRIERS.

The biggest deterrent to complying with cybersecurity guidelines is remembering a random sequence of letters, numbers and symbols. If a new password is difficult to remember, train people to create complex passwords they can remember even if they are not linked to personal information—iLove25leep247! And pick something that makes you happy, because bundling something positive with something negative is the best way to make the negative less negative.

Dr. Keller is a professor of marketing at Dartmouth College's Tuck School of Business in Hanover, N.H. She can be reached at reports@wsj.com.