I Know All the Rules About Cybersecurity. Yet I Still Break Them.

The reasons say a lot about what's wrong with the rules, and how to make us safer Monday, June 22, 2020 | R7 JOURNAL REPORT | CYBERSECURITY social media was the lifeline that kept us connected, and now it feels even more important to share our family's joys online and get support when we have moments of grief and frustration. Make it easier: Social-networking platforms need to make it easier for us to narrow or widen the audience for our posts. Setting up per- missions for who can see what con- tent takes a fair bit of grooming and tweaking, and many platforms don't even give you that option.

Social networks should also de- fault to a high level of privacy for new users or for kid-related content, we can get something for nothing— that online publications and social networks should be free. When consumers balk at paying for online services, it is easier for service providers to just fall back on the proven tactic of mining our data and selling our eyeballs to the highest bidder.

Instead, social networks and other web services should all offer the option of buying our freedom back by paying a monthly service charge to get content and interactions, and not see ads or have our data mined. (After all, many of us happily pay to upgrade favorite mobile apps to their ad-free versions.) The rule: Regularly back up your devices to an external hard drive— ideally two of them, so that no matter what goes wrong at home or in the cloud, you'll have your data.

Why I break it: No matter how many times I set my computer up to back up over Wi-Fi, it fails—so I once again find myself backing up over a cable connection, which is just too cumbersome and space-intensive to do regularly. Plus, I keep so much of my life in Dropbox, Google Drive and Gmail that 95% of my current working files are retrievable anyhow.

Make it easier: Backing up an entire computer should be as easy as back- ing up individual files to Dropbox or Google Drive. Just let us check the parts of our computer we want to sync—or select the entire hard drive. That way, we not only back up all our crucial files regularly but also other critical things few people think about backing up: our personalized settings and applications.

The rule: Use two- factor authentication wherever possible, so that your sign-on has to be confirmed by phone, text or another method. Why I break it: Two-factor authentication is inconvenient and annoying. You need to wait for the authentication code to arrive, and if you can't find your phone immediately, you end up hunting for it just so that you can log in to a website on your computer. Meanwhile, certain apps that handle verification may lock you out if you switch to a new phone.

Make it easier: The industry should adopt the painless verification that some apps use—letting me confirm my identity immediately through the app itself. For instance, if you have the Gmail app on your phone and try to sign in somewhere else, a message pops up from the Gmail app asking, "Is this you?", so nobody can sign into your Gmail account unless they can confirm that login on your phone. (Another good reason to keep your phone face, fingerprint or password protected!) It is far less convenient to wait for (and type in) a verification code. Messing around with text-messaged codes should be a fallback scenario, not the default behavior.

Dr. Samuel is a technology researcher and the author of "Work Smarter with Social Media." She can be reached at reports@wsj.com. BY ALEXANDRA SAMUEL

We all know we're supposed to follow basic cybersecurity practices like using a pass- word manager or running antivirus software— just the way we know we're sup- posed to floss every day and keep eight months of emergency savings in the bank.

Being human, however, we of- ten fall short. And even though I've been researching and writing about cybersecurity for more than two decades, I'm no exception. I'm just as likely as anyone to cut corners on my own online security.

If a geek like me doesn't follow the rules, can we really expect normal people to do it?
What follows are some of the rules I break, and why I break them. They offer a glimpse at what's wrong with cybersecurity these days and what needs to happen so that more people will follow the rules, and be safer online.

The rule: Generate and keep all your passwords in a password manager so that you use only unique, complex passwords.

Why I break it: Password managers seem like a great idea. They are dedicated apps that store all your passwords in one place and fill them in when you visit a site, so you don't have to remember them or retype them each time. You can import your current passwords, or let the apps generate new and complex ones for you. And you can access the apps from different devices and applications.

In practice, however, these apps can be somewhat inconvenient. On some websites, the password manager may not be able to detect which password to use, and some apps or devices make it hard to access the man- ager in the first place. I also run into trouble with duplicate passwords. I've got multiple password managers—the one I chose because it works across all my devices and applications, and the other ones that just came bundled with my system or web browser. When I go to a site, any or all of these managers will ask me if I want to save or update my login—so if I'm not paying close attention, it's easy for me to save my password to the wrong app, and then forget where I put it. Or I end up with one manager that has my current password, and another one with an out-of-date login.

Then if I return to the site, I have to hunt through all these different password managers to find the one with the right password or just give up, create a new password, and have even more password versions to contend with. Even my dedicated password manager can end up with duplicate passwords, because it's easy to screw up and accidentally choose to create a new password when I'm just trying to update an existing one, which means I end up with duplicates for certain sites. Then I have to figure out which of my five different Gmail logins is the actual current version.

For this reason, I don't rely on my password manager for services like Facebook, Twitter and Google. Lots of sites let you use those services to log in, instead of creating new accounts on the site itself. Since I choose that option frequently, it's easier just to remember the passwords for those big, useful accounts—which I call "keychain" logins—rather than fiddle with the pass- word manager and fix its mistakes.

Make it easier: Give me one password option to rule them all. Once I install a password manager on a device, my browsers and operating system should know to store my passwords there, instead of prompting me to use their own systems. And please, test those pass- word managers in the field, with a wider range of actual users.

The rule: Don't over-disclose on social media, which creates personal and professional vulnerabilities online and offline, especially for children.

Why I break it: I don't have a lot of opportunity to get out and socialize, and many of my dearest friends live far away. Even before Covid19, so instead of extreme openness that only tech nerds know how to limit. Rather than assuming that every new social-media connection is a true friend who gets access to my entire life, put everyone on the equivalent of my restricted list until I deliberately admit them to my inner circle.

The rule: Use an ad blocker and decline cookies so that you won't be tracked across multiple websites or get ads targeted to your personal browsing history.

Why I break it: Many media sites prevent you from accessing their content if you're using an ad blocker, because it kills their main source of revenue. And declining cookies just means that I get a thousand irrelevant ads for belly-fat busters, when I could be seeing relevant ads for red cowboy boots, patio furniture and coding games. If I have to see ads, they might as well be tailored ones.

Make it easier: Targeted ads are a ubiquitous part of the browsing experience because many of us are still laboring under the illusion that Security measures can be inconvenient, annoying and too restrictive.

What Keeps Me Up at Night "In the wake of Covid-19, attackers are taking advantage of the increase in remote workers and are preying on the fear of individuals with Covid19themed scams....In addition to adjusting some of our security protocols, we have also accelerated some of our security road map plans. This includes many practices, from increased software updates, to employee training and awareness, to implementing a zero-trust security model [which requires verification each time anyone seeks access to a network, with no exceptions]....Whether our employees are working from the office, their home or the local coffee shop, you need to make sure the devices are safe and updated for ongoing threats." Olivier Leonetti, chief information officer and chief financial officer, Zebra Technologies Corp.