Building a Better Password

Tough to remember but easy to crack, passwords are the weak link in computer security. Billions hang in the balance.

By Nick Summers | NEWSWEEK

Published Oct 9, 2009

From the magazine issue dated Oct 19, 2009

My password is gr8199. I've been using it for more than a decade, ever since a Web site first required me to create a string of six to 12 characters, with a mixture of letters and numbers. At that moment the only sequence I could think of had to do with the Wayne Gretzky vanity license plate my family happened to be considering: the Great One, No. 99, which yielded gr8199. As the requirements for passwords evolved over the years, I added extra nines, cobbled on a question mark, and blended it with my alternate password (which is, insanely, my Social Security number). Until last week, gr8199 and its descendants got you into my laptop, my e-mail, my Scrabble, my bank accounts, my blog, my work PC, my health insurance, Facebook, Skype, Snapfish, Hulu, my tax returns, and at least 39 other sites across the Internet. I can tell you my secret code because I'm changing it; I'm changing it because I'm telling you. My password system is a mess—and I bet yours is, too.

If you're a typical Web user—and these days, what office worker doesn't spend all day plugged in to the browser?—you have 6.5 passwords, each of which is used at four sites, and you're forced to type one eight times per day. Your employer likely makes you create a brand-new code every 90 days. At one point or another, you've probably scrawled a password on a Post-it, e-mailed one to yourself, or made other security-breaching concessions to the fundamental impossibility of memorizing so many strings of gobbledygook. Today we don't have passwords so much as coping systems.

Companies spend billions of dollars protecting their computer systems, and passwords are a linchpin. With so much riding on Americans' faulty passwords, there has to be a better way to make our technology secure—and it's taking shape inside Carnegie Mellon University's cyber-security-research department. There is no password 2.0 in the wings, no genius breakthrough to secure our stuff forever. But for the past five years a few members of CyLab, as it's known, have been studying not just the mathematical theory behind passwords but the way humans actually use them. Their findings suggest there's a lot we can do to make this part of our lives far less of a hassle—and in my case, to move far beyond gr8199.

Though it's housed in an otherwise nondescript building on the north side of Carnegie Mellon's Pittsburgh campus, parts of CyLab resemble James Bond's Q Branch. The biometrics lab in particular is hard at work taking the fiction out of science-fiction movies like *Minority Report*.

The workspace is a hive of activity, with 15 students bent over all manner of gadgetry; it's like a high-school shop class, but with prototype face-tracking cameras instead of band saws. This is where Carnegie Mellon wows its visitors, with toys that can read a person's fingerprint from across the room, reverse-engineer a 3-D model of a face from a simple 2-D snapshot, and recognize a moving iris at 13 meters. Nearly every gadget here would give a civil libertarian a stroke.

With their futuristic sexiness and fat military funding, biometrics and bleeding-edge cryptography have long drawn the best minds in computer security. But for average consumers, biometrics has also been among the biggest letdowns in security. The fingerprint scanners available on some laptops are essentially novelties, for example, and voice authentication has never been reliable or secure enough to function on its own. Cost is also a huge obstacle: unless you work at the CIA, your employer isn't likely to buy you an iris reader any time soon. "Biometrics never caught on, and it never will," says Richard Power, a CyLab fellow who rails about the lack of progress—he calls it a "lost decade"—in computer security.

For regular people accessing Web sites and PCs, passwords are what we're stuck with, primarily because they're simple and cheap. Among computer researchers, passwords are a key aspect of a burgeoning field known as "usable security." At Carnegie Mellon, the scientists who've pioneered the discipline work not in a lab but upstairs in a wing that looks no different from most universities' English or history departments. Look closer, though, and you'll see signs that this is no ordinary place. The doors are all marked with 2-D bar codes; a professor enters his office by snapping a photo with his cell phone. *Click!* goes the phone; *thunk!* slides the bolt. It's more secure than a physical key, which can be stolen and copied, and no less handy.

The academics here are rethinking basic questions about what makes something—an office, a Web site—secure, without driving its owner crazy. And their findings call into question many of the recent security advances in the banking, e-mail, and other critical systems you log into every day. Researchers here fault virtually everything your corporate IT department tells you about strong passwords. And they take the radical stance that you, the user, should be listened to when passwords become overbearing, not yelled at when you forget them.

As an academic discipline, usable security—a blend of computer science and psychology—is only about five years old. "When we first started waving the flag, not many people paid attention," says Carnegie Mellon professor Lorrie Cranor. "It's gratifying that people are starting to." Cranor may be more responsible than anyone else for establishing the field. She founded CyLab's Usable Privacy and Security Laboratory and an annual symposium; she also edited the major textbook on the subject and teaches one of the few usable-security-specific courses in the nation. Polite and warm, Cranor strives to be user-friendly herself: when she gets too technical while describing her work to a decidedly non-Ph.D. NEWSWEEK reporter, she pauses, laughs ("Were you expecting a more usable definition?"), and resumes the discussion in geek-free English. Her interest in patterns and complexity extends outside the lab: she's a master quilter whose designs have been featured on the covers of textbooks and journals.

Much of Cranor's work involves poking holes in the conventional wisdom about how users should choose and remember passwords. Take one common tip that Internet users hear: to make a super-strong password, think of a phrase, and string together the first letter of each word. The result is called a mnemonic password. The famous *Ghostbusters* line "Dogs and cats, living

together!" becomes, with a few substitutions, "D&c,lt!"—a sequence to make an IT director swoon. It's easy to remember, and who could guess it?

In fact, Cranor can. In a 2006 study, her team asked 144 volunteers to come up with mnemonic passwords. Guessing that the subjects would summon well-known phrases from memory, the researchers built a simple program to crawl the Web for famous quotes, ad slogans, song lyrics, and nursery rhymes, quickly amassing 249,000 entries. By security standards, that's a relatively small universe of phrases upon which to base passwords. Using that list, their crude program cracked 4 percent of the mnemonics, which weren't so unique after all—two subjects chose the Oscar Mayer wiener jingle—suggesting that motivated hackers could fare even better.

Instead of a mnemonic password, research suggests that users are better off constructing passwords out of the phrase itself—a passphrase. As the technologist Thomas Baekdal notes, a short but hard-to-remember string like "J4fS<2" can be broken by what is called a brute-force attack (in which a computer attempts "a," then "ab," then "abc," and so on) in 219 years, while a long but easy-to-remember phrase like "du-bi-du-bi-dub" will stand for 531,855,448,467 years. (Two hundred nineteen years is actually very good, but the lesson remains: simpler can be stronger.) The idea of passphrases isn't new. But no one has ever told you about it, because over the years, complexity—mandating a mix of letters, numbers, and punctuation that AT&T researcher William Cheswick derides as "eye-of-newt, witches'-brew password fascism"—somehow became the sole determinant of password strength.

What drives Cheswick and other researchers particularly nuts is that the "dictionary" attacks that these complicated passwords are supposed to repel have been largely supplanted by "phishing," which tricks users through deceptive e-mails and look-alike Web sites into unwittingly handing over passwords directly to hackers. For all the hoops the users have to jump through, researchers say they're mostly fighting the last war. "Users have this secret feeling that they don't need these rules, and they're right," says Cheswick, who is known as one of the fathers of Internet security.

That hasn't stopped Web sites from continuing to foist increasingly complex requirements on users. And a natural consequence of passwords that are more complicated, and that require periodic resets, is that people forget them more frequently. To deal with that, many sites—notably free Web e-mail services—have adopted "security questions" such as "Where did you go to elementary school?" and "What is your pet's name?" In theory, answering such questions proves that you are you. In practice, it's riddled with flaws. Last fall, Sarah Palin's personal e-mail account, gov.palin@yahoo.com, was hacked by a student in Tennessee who knew from rudimentary Web searches her birth date, ZIP code, and that she had met her husband in high school. And in July, Twitter executives were embarrassed by a similar attack, which resulted in the theft of some 300 internal documents, including strategy memos and financial forecasts. A May 2009 study from Microsoft Research and Carnegie Mellon eviscerated the -security-question strategies employed by three of the top four Web-mail providers, finding that subjects could guess their acquaintances' AOL and Yahoo challenges more than a quarter of the time. Hacking isn't the only problem caused by the spread of these questions: according to the study, one in five subjects forgot the answers to their own questions in six months.

One way humans deal with password overload is to rely on a single password and simple variants for nearly every electronic interface in their lives—as I did. That's highly problematic because if that all-powerful password is cracked at just one site, it gives a hacker the keys to the kingdom. That's why Adrian Perrig, the technical director at Carnegie Mellon's CyLab, promotes disposable passwords: generated by special devices, people use these passwords once, then throw them away. It used to be expensive for companies to give employees special fobs that could synchronize with a server and make one-time passwords possible, but nowadays we all carry a device capable of this task: a cell phone. RSA, the company that manufactured the most recognizable model of password fob, now bakes the technology directly into BlackBerrys.

Perrig's scheme is dubbed Phoolproof Phishing Prevention. Using this system, a user enters his log-in name at a given site, and in a moment, his phone beeps with a text message containing a temporary password. A criminal can steal your password silently. But if he snatches your cell phone, you'll know right away. Another benefit: if a hacker is listening in on an unsecured wireless network, or through a nasty piece of malware called a keylogger, the password is no good after the one session. Last December, Bank of America became the first major U.S. bank to let customers link mobile phones (or, for $20, a wallet-size card) to their accounts, a breakthrough in Internet banking. So far, though, only a fraction of customers have opted in.

Another promising direction might be image-based passwords. No, not that personalized icon that greets your log-in at Bank of America, Vanguard, and many other banking sites; it's a nice marketing trick, but has little security benefit. "We saw that and laughed at it right from the beginning," says Cranor; one study showed that all a phisher needed to do was insert a sentence like "Our image server is down; please log in anyway" into a fake Web page, and people would do so. Paul van Oorschot, a professor of computer science at Carle-ton University in Ottawa, has developed schemes that replace text entry with mouse clicks on certain pixels in an image—say, the headlight of a sports car. This approach has flaws, usable-security proponents say, and hasn't been tested enough. But it's cheap, and resistant to phishing.

As often happens with academic research, it has taken some time for the industry to take notice. But lately, people inside tech companies have begun paying more attention to the usable-security work being done at Carnegie Mellon and elsewhere. Cormac Herley, a Ph.D. at Microsoft Research, recently published two papers questioning the industry's accepted wisdom on security: "Do Strong Web Passwords Accomplish Anything?" (conclusion: sometimes, but not really) and "Passwords: If We're So Smart, Why Are We Still Using Them?" The latter paper concludes that in the short to medium term, passwords, flawed as they are, are here to stay. "Right now, we all agree that the password system is terrible, yet how much money is it costing companies?" van Oorschot asks. "Are they feeling enough pain that they're willing to do anything about it?"

For now, the answer is no. And as Bank of America's customers have shown, even if a more secure option exists, many won't opt for it. But as time goes on, the combination of a major security breach and users' growing fatigue at juggling so many passwords will likely make the world more receptive to the innovations being cooked up at Carnegie Mellon. Until then, we'll all have to keep on trying to remember our own variations of gr8199.