Farhad Manjoo

Fix Your Terrible, Insecure Passwords

in Five Minutes

Farhad Manjoo is the technology columnist for *Slate* and is

also a frequent contributor to the *New York Times*. After

graduating from Cornell University in 2000, where he served

as editor-in-chief of the *Cornell Daily Sun*, Manjoo wrote for

both *Wired News* and *Salon.com* before his current position

at *Slate* (where this essay appeared in 2009). He makes

regular appearances on National Public Radio and is also

the author of *True Enough: Learning to Live in a Post-fact*

*Society* (2008).

GUIDING QUESTION

Why are most passwords at risk?

It is tempting to blame the victim. In May, a twenty-something French

hacker broke into several Twitter employees’ e-mail accounts and stole

a trove**1** of meeting notes, strategy documents, and other confidential

scribbles. The hacker eventually gave the stash to TechCrunch, which has

since published notes from meetings in which Twitter execs discussed

their very lofty goals. (The company wants to be the first Web service to

reach 1 billion users.) How did the hacker get all this stuff ? Like a lot of

tech startups, Twitter runs without paper — much of the company’s discussions

take place in e-mail and over shared Google documents. All of

these corporate secrets are kept secure with a very thin wall of protection:

The employees’ passwords, which the intruder managed to guess because

some people at Twitter used the same passwords for many different sites.

In other words, Twitter had it coming. The trouble is, so do the rest of us.

Your passwords are not very secure. Even if you think they are, they probably

aren’t. Do you use the same or similar passwords for several different

important sites? If you don’t, pat yourself on the back; if you do, you’re not

alone — one recent survey found that half of people online use the same

password for all the sites they visit. Do you change your passwords often?

Probably not; more than 90 percent don’t. If one of your accounts falls to a

hacker, will he find enough to get into your other accounts? For a scare, try

this: Search your e-mail for some of your own passwords. You will probably

find a lot of them, either because you’ve e-mailed them to yourself or because

some Web sites send along your password when you register or when you tell

them you have forgotten it. If an attacker manages to get into your e-mail,

he’ll have an easy time accessing your bank account, your social networking

sites, and your fantasy baseball**2** roster. That’s exactly what happened at Twitter.

(Here’s my detailed explanation of how Twitter got compromised.)

Everyone knows it’s bad to use the same password for different sites.

People do it anyway because remembering different passwords is annoying.

Remembering different difficult passwords is even more annoying.

Eric Thompson, the founder of AccessData, a technology forensics company

that makes password-guessing software, says that most passwords

follow a pattern. First, people choose a readable word as a base for the

password — not necessarily something in *Webster’s***3** but something that is

pronounceable in English. Then, when pressed to add a numeral or symbol

to make the password more secure, most people add a 1 or ! to the end

of that word. Thompson’s software, which uses a “brute force” technique

that tries thousands of passwords until it guesses yours correctly, can easily

**1. trove:** valuable collection **2. fantasy baseball:** an online game where players

manage players and compete against each other **3. Webster’s:** a

well-known dictionary

Readings for writers

suss out**4** such common passwords. When it incorporates your computer’s

Web history in its algorithm**5** — all your ramblings on Twitter, Facebook,

and elsewhere — Thompson’s software can come up with a list of passwords

that is highly likely to include yours. (He doesn’t use it for nefarious

ends; AccessData usually guesses passwords under the direction of a court

order, for military purposes, or when companies get locked out of their

own systems — “systems administrator gets hit by a bus on the way to

work,” Thompson says by way of example.)

Security expert Bruce Schneier writes about passwords often, and he

distills Thompson’s findings into a few rules: Choose a password that

doesn’t contain a readable word. Mix upper and lower case. Use a number

or symbol in the middle of the word, not on the end. Don’t just use 1 or

!, and don’t use symbols as replacements for letters, such as @ for a lowercase

A — password-guessing software can see through that trick. And of

course, create unique passwords for your different sites.

That all sounds difficult and time-consuming. It doesn’t have to be. In

Schneier’s comment section, I found a foolproof technique to create passwords

that are near-impossible to crack yet easy to remember. Even better,

it will take just five minutes of your time. Ready?

First, start with an original but memorable phrase. For this exercise,

let’s use these two sentences: *I like to eat bagels at the airport* and *My first*

*Cadillac was a real lemon so I bought a Toyota*. The phrase can have something

to do with your life or it can be a random collection of words — just

make sure it’s something you can remember. That’s the key: Because a

mnemonic**6** is easy to remember, you don’t have to write it down anywhere.

(If you can’t remember it without writing it down, it’s not a good

mnemonic.) This reduces the chance that someone will guess it if he gets

into your computer or your e-mail. What’s more, a relatively simple mnemonic

can be turned into a fanatically difficult password.

Which brings us to Step 2: Turn your phrase into an acronym. Be sure

to use some numbers and symbols and capital letters, too. *I like to eat*

*bagels at the airport* becomes *Ilteb@ta*, and *My first Cadillac was a real lemon*

*so I bought a Toyota* is *M1stCwarlsIbaT*.

That’s it — you’re done. These mnemonic passwords are hard to forget,

but they contain no guessable English words. You can even create pass

phrases for specific sites that are coded with a hint about their purpose. A

sentence like *It’s 20 degrees in February, so I use Gmail* lets you set a new

Gmail password every month and still never forget it: *i90diSsIuG* for September,

*i30diMsIuG* for March, etc. (These aren’t realistic temperatures;

they’re the month-number multiplied by 10.)

**4. suss out:** investigate **5. algorithm:** a step-by-step process for solving a

problem **6. mnemonic:** a way to assist memory

How many different such passwords do you need? Four or five at

most. You don’t have to keep unique passwords for every single site you

visit — Thompson says it’s perfectly OK to repeat passwords on sites that

don’t need to be kept very secure. For instance, I can use the same password

for my accounts at the *New York Times*, the *New Republic*, *The New*

*Yorker*, and other online magazines, because it won’t hurt me too much if

someone breaks into those. (My mnemonic is, *I like to read snooty publications*

*quite often.*) You should probably use different passwords for each of

your social networking accounts — someone can do real damage by breaking

into your Facebook or Twitter, so you want to keep them distinct — but

you can still come up with a single systematic mnemonic to protect them:

*Twitter is my second favorite social networking site, MySpace is my third favorite*

*social networking site*, etc. Reserve your strongest, most distinct passwords

for the few very important services that, if cracked, could do the most

damage — your bank account, your computer, and most of all your e-mail,

which often contains the keys to everything else in your life.

To be sure, this is more of a hassle than what you’re doing now — but

what you’re doing now is going to come back to bite you. These days,

we’re all dishing personal information all the time; you may think that

your password is totally unguessable, but your Facebook makes clear that

you’re a huge U2 fan and you graduated from college in 2000. *Achtung2000*,

eh? Just go ahead and make some new passwords right now.

Trust me, you’ll feel better.

SUMMARIZE AND RESPOND

In your reading journal or elsewhere, summarize the main point of “Fix Your

Terrible, Insecure Passwords in Five Minutes.” Then, go back and check off

support for this main idea. Next, write a brief summary (three to five sentences)

of the essay. Finally, jot down your initial response to the essay. Manjoo

thinks this is an urgent problem: He urges his readers to change their

passwords immediately. Do you see password security and online privacy

protection as pressing issues? Does this essay change your view of them?

CHECK YOUR COMPREHENSION

1. Which of the following would be the best alternative title for this

essay?

a. “How the Internet Is Changing Our Society”

b. “Safeguarding Your Internet Passwords in Two Easy Steps”

c. “We Need Stronger Laws to Punish Hackers”

d. “Don’t Put Personal Information on the Internet”

9

10

Pause: What kind of

“damage” is Manjoo

referring to in this

paragraph?

45\_ANK\_48084\_Ch44\_733-746.indd 739 11/16/11 8:27 AM

Readings for writers

740 Chapter 44 • Process Analysis

2. The main idea of this essay is that

a. people are spending too much time online and neglecting direct

human relationships.

b. the government needs to do more to protect people’s online

security from hackers.

c. people need to choose better online passwords and that it’s

easy for them to do so.

d. popular sites such as Facebook and Twitter deserve to be

hacked.

3. According to the author, most people should

a. have only one password for all their Internet accounts, preferably

a readable word that doesn’t mix upper and lower case

letters.

b. have four or five different passwords at most.

c. have a separate password for every online account and site.

d. avoid shopping, networking, or banking online altogether

because these activities are too risky.

4. If you are unfamiliar with the following words, use a dictionary to

check their meanings: hacker (para. 1); roster (2); forensics, nefarious

(3); distills (4); random (6); acronym (7).

READ CRITICALLY

1. Why does Manjoo begin with the story about Twitter? How does it

support his overall purpose?

2. Where in the essay does the writer rely on experts? What do they

contribute to Manjoo’s main point?

3. How does Manjoo use examples to detail the steps of his process?

Do you find them helpful?

4. In paragraph 9, the writer gives suggestions for how and when to

use different online passwords. What order does he use to structure

this advice?

5. After reading this essay, will you change your Internet passwords?

Will you use Manjoo’s method? Why or why not?