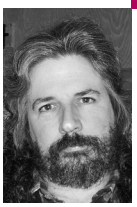
ROBERT G. FERRELL

/dev/random: five common misconceptions about information security



Robert G. Ferrell is an information security geek biding his time until that genius grant finally comes through.

rgferrell@gmail.com

1. TELNET IS INSECURE.

Telnet is just another protocol. It is no more "insecure" than leaving a loaded revolver with no safety in the nursery is "irresponsible." If you're worried about passwords being transmitted in clear text, just disable authentication altogether. Problem solved. Stop sniffling, you big baby. Port 23 is your friend.

2. Botnets will steal your identity.

Worrying about your identity being stolen by malicious software on your computer is perfectly valid. The malicious software in question will not be installed surreptitiously as a result of an ill-advised visit to a hacked Web site, however. It will be installed by you or your computer's retailer in the form of a Web browser. The likelihood is that the culprit will obtain your information from a "trusted" company's hacked database or stolen laptop/backup media/USB device, not some vast network of hapless zombie computers. Botnets run a distant second to misplaced trust and good ol' fashioned physical larceny.

3. Increasing the number of characters in your password makes it more secure.

The concept of diminishing marginal returns, which I vaguely recall from a macroeconomics class in college in 1978, has never been more clearly demonstrated (does it bother you that "demonstrate" contains "demons"? It does me) than with institutions who keep jacking up password length in the badly mistaken belief that this increases security. Human beings, especially those brought up in a 60-spasmodically-disjointed-images-in-a-30-second-commercial world, have considerable difficulty retaining anything longer than three or four characters. This memory shortfall is further exacerbated by the ubiquity of portable data storage devices and speed dial lists. Presented with a 12 or 14 member string of more or less arbitrary characters they are told they must regurgitate in order to log on, it is absolutely guaranteed that the vast, vast majority of people will at some point commit that password to paper or non-volatile electronic memory. Unless this written record is now scrupulously stored in a safe or equivalent environment at all times, the security of that system just plummeted precipitously. Add to that the fact that it has recently been shown that 14-character password hashes meeting industry standard complexity requirements can be broken by optimized Rainbow Tables in under 6 seconds on a mediocre processor, and it should be fairly apparent that

relying solely on longer passwords in fact dramatically decreases data confidentiality. Oh, and just for the record, "two-factor authentication" does *not* mean "user ID and password."

4. Antivirus software will keep my computer secure.

This is a load of fetid dingo kidneys, to borrow one of my favorite phrases from the late Douglas Adams. I will clarify my point with a metaphorical examination of exactly how signature-based antivirus software works. Let's say you're a contracted bouncer at a popular club. You have a list of the names of people not allowed to come in and, because we're really trying to be secure here, a physical description of each. Now, so long as the people you're trying to keep out don't give you a false name and change their appearance, this filtration system works pretty well. However, it is in the nature of people who are likely to end up on a "no-entry" list to be duplicitous, so the efficacy of this approach is somewhat less than optimal. Not to worry, though—you can watch the guests and eject any whose actions are suspect. Or, rather, you could if that part of your behavioral repertoire hadn't been disabled by an employer who makes most of its money from selling no-entry list subscriptions to clubs. If you can simply throw out the bad apples, why would club management need to spend money on a new list of miscreants every week?

To recap, antivirus software keeps your computer secure so long as it only encounters well-known malware that makes no effort to disguise itself. This practice goes hand in hand with the usual operating system–supplied firewall that blocks everything except the email and Web traffic where 99% of all malicious software of concern to the average user originates. Congratulations, your illusion of security is now complete. Don't forget to take your blue pill every morning.

5. A Nigerian government official wants to give you money.

I honestly thought this threat would go the way of smallpox and the American ivory-billed woodpecker as an increasingly connected world facilitated the widespread dissemination of warnings thereto appertaining. No one ever lost money overestimating human greed and ignorance, though. Repeat after me: I will never, ever, under any circumstances be asked to help an actual corrupt official of an actual sub-Saharan African nation launder 37 million dollars, for one simple reason: they don't have that kind of money. Even if they did, it would be going to buy private jets and Mediterranean vacation homes for ruthless dictators, not sitting unnoticed in some forgotten bank account waiting to be slipped quietly to an avaricious idiot in the U.S. Even Third World nations have government auditors. The same goes for international lotteries based on random email addresses, scam victims reimbursement funds, intestate wealthy persons tragically killed in transportation disasters, and kindly old women dying of cancer who want total strangers to invest their sizeable fortunes in charitable causes on their behalf. The single most useful dictum I learned in that college economics class was TANSTAAFL: *There Ain't No Such Thing As A Free Lunch*. Ferrell's First Law of Fiscal Dynamics states that money does not fall from the sky, nor does it flow freely from regions of low concentration to regions of high concentration without the application of reverse monetary osmosis (also known as international commerce). Large sums of money are Luddite in nature: they tend to announce themselves with certified snail mail, not SMTP. If an offer seems too good to be true, at least you're paying attention.

Keeping computers reasonably secure is akin to fending off flies in defense of a dung pile. The job is a lot easier if you patch those gaping holes in your fly swatter.

And hold your nose.