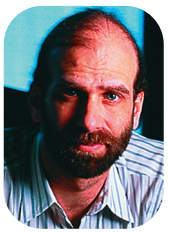
Authentication and Expiration

There's a security problem with many Internet authentication systems that's never talked about: there's no way to terminate the authentication.



Bruce Schneier
Counterpane Internet Security

A couple of months ago, I bought something from an e-commerce site. At the checkout page, I wasn't able to just type in my credit-card number and make my purchase. Instead, I had to choose a username and password. Usually I don't like doing that, but in this case I wanted to be able to access my account at a later date. In fact, the password was useful because I needed to return an item I purchased.

Months have passed, and I no longer want an ongoing relationship with the e-commerce site. I don't want a username and password. I don't want them to have my credit-card number on file. I've received my purchase, I'm happy, and I'm done. But because that username and password have no expiration date associated with them, they never end. It's not a subscription service, so there's no mechanism to sever the relationship. I will have access to that e-commerce site for as long as it remembers that username and password.

In other words, I am liable for that account forever.

Traditionally, passwords have indicated an ongoing relationship between a user and some computer service. Sometimes it's a company employee and the company's servers. Sometimes it's an account and an ISP. In both cases, both parties want to continue the relationship, so expiring a password and then forcing the user to choose another is a matter of security.

In cases with this ongoing relationship, the security consideration is damage minimization. Nobody wants some bad guy to learn the password, and everyone wants to minimize the amount of damage he can do if he does. Regularly changing your password is a solution to that problem.

This approach works because both sides want it to; they both want to keep the authentication system working correctly, and minimize attacks.

In the case of the e-commerce site, the interests are much more one-sided. The e-commerce site wants me to live in their database forever. They want to market to me, and entice me to come back. They want to sell my information. (This is the kind of information that might be buried in the privacy policy or terms of service, but no one reads those because they're unreadable. And all bets are off if the company changes hands.)

There's nothing I can do about this, but a username and password that never expire is another matter entirely. The e-commerce site wants me to establish an account because it increases the chances that I'll use them again. But I want a way to terminate the business relationship, a way to say: "I am no longer taking responsibility for items purchased using that username and password."

Near as I can tell, the username and password I typed into that e-commerce site puts my credit card at risk until it expires. If the e-commerce site uses a system that debits amounts from my checking account whenever I place an order, I could be at risk forever. (The US has legal liability limits, but they're not that useful. According to Regulation E, the electronic transfers regulation, a fraudulent transaction must be reported within two days to cap liability at US$50; within 60 days, it's capped at $500. Beyond that, you're out of luck.)

This is wrong. Every e-commerce site should have a way to purchase items without establishing a username and password. I like sites that allow me to make a purchase as a "guest," without setting up an account.

But just as importantly, every e-commerce site should have a way for customers to terminate their accounts and should allow them to delete their usernames and passwords from the system. It's okay to market to previous customers. It's not okay to needlessly put them at financial risk.

Bruce Schneier *is one of the world's foremost security experts and chief technical officer of Counterpane Internet Security. His most recent book is* Beyond Fear: Thinking Sensibly about Security in an Uncertain World. *You can subscribe to his email newsletter,* Crypto-Gram, *at www.schneier.com.*

Ed. Note: Another version of this column appears in Schneier's Crypto-Gram newsletter.