Many hands make security work

Effective identity protection should encompass a mixture of methods, not only user-education

BY STEPHEN WILSON

If one thinks about online security for a minute, all sorts of parallels emerge with other fields. A favourite comparison of mine is with road safety. Like all metaphors, it's risky to overdo it, but the point I want to make is that like road safety, effective online security must involve a blend of user education, standards, processes, and technological innovation.

In my view, online safety is poorly served by an obsession with user education. Numerous governments and industry groups have developed reams of technically reasonable security advice; see for example www.protectfinancialid.org.au or www.staysmartonline.gov.au. But in truth this material is overwhelming. The subtle implications are that security is for experts, and that the Internet isn't safe unless you go to extremes. Moreover, the most recent attacks show that even if consumers do their best online, their personal details can still be taken over by massed raids on merchant databases.

So is it fair to place the onus so heavily on regular users for protecting their identities online? In 2005, in response to a wave of phishing attacks, eBay's Hani Durzi said "I know that it sounds very basic, but education is the silver bullet". Yet nobody would be so simplistic about road safety. As a community we accept that road safety rests evenly on enforceable road rules, legislated standards, quality automotive products, sophisticated traffic systems, and driver training and licensing. Education alone would be worthless.

In the recent aftermath of the TJX disaster (where tens of millions of credit card numbers were stolen by a gang that infiltrated department store networks), I came across a provocative headline: "Preventing data breaches not a technology issue". At the risk of political incorrectness, I say that's ridiculous. It's like claiming that preventing bank robbers is not a technology issue.

Credit card fraud and ID theft in general are in dire need of concerted technological responses. Our card-not-present payments processing arrangements were developed many years ago for mail orders and telephone orders. It was perfectly natural to coopt the same processes when the Internet arose, since it seemed to be yet another communications medium. But the Net turned out to be more than an extra channel: it connects everyone to everything, around the clock.

The Internet has given criminals x-ray vision into almost everyone's banking details, and perfect digital disguises with which to defraud online merchants. There are opportunities for crime now that are quantitatively and qualitatively radically different from what went before. In particular, because identity data is available by the terabyte and digital data has no respect for originals versus copies, identity takeover is child's play.

You don't even need to have ever shopped online to run afoul of CNP fraud. It is now apparent from TJX and other cases that most stolen credit card numbers are obtained en masse by criminals invading databases at merchants' back-ends. These attacks go on behind the scenes, out of sight of even the most careful customers.

So the standard online security advice increasingly misses the point. Consumers are told earnestly to look out for the SSL padlock that purportedly marks a site as "secure". They're supposed to have firewalls and to keep their PCs patched and up-to-date. They're advised to only shop online at reputable merchants and to avoid suspicious looking sites (as if cyber criminals aren't sufficiently organised to copy legitimate sites in their entirety). None of this advice touches on the real source of illicit identity data.

Merchants too are on the hook for increasingly unwieldy and futile security overheads. When a business wishes to accept credit card payments, it's fair enough in the real world that they install certified terminal equipment. But to process credit cards online, shopkeepers now have to sign up to onerous PCI requirements that in effect require even SMEs become IT security specialists. And to what end? No audit regime will ever stop organised crime. To stem identity theft, we need to make stolen IDs less valuable.

All this points to urgent public policy matters for government and banks. It is not enough to put the onus on individuals to guard against one-off personal attacks on their credit cards. Systemic changes and technological innovation are needed to render stolen personal data useless to thieves. It's not that the whole payments processing system is broken; rather, it is vulnerable at one or two specific points, because cyber criminals have figured out how to pick the locks.

> To stem identity theft, we need to make stolen IDs less valuable

Digital identities are literally the keys to our valuables. As such they really need to be treated as seriously as house keys and car keys. These things have become very high tech indeed. Modern car keys cannot be duplicated at a suburban locksmith; some office and filing cabinet keys even carry government security certifications. And we never use the same keys for our homes and offices; we wouldn't even consider it (but think about that for a moment and compare it to the craze for Single Sign On).

There has been almost no comparable attention given to protecting digital identities as keys. Our technology neutrality and regulatory timidity has led to a bewildering array of stop-gap authentication approaches; at the same time we've done nothing to inhibit the re-use of stolen ID data. It's high time that all sectors reliant on the online channel got working together on a uniform and universal set of smart identity tools to protect consumers online.

Stephen Wilson is a leading international authority on identity management and information security. In early 2004, Stephen established Lockstep Consulting to provide independent security advice and to develop new smartcard solutions to identity theft.

swilson@lockstep.com.au