Identity Theft (2): The Shadowcrew Case

by M. E. Kabay, PhD, CISSP-ISSMP
CTO, School of Graduate Studies
Norwich University, Northfield VT

In my last column in this series on identity theft, I introduced some statistical resources about the problem. Today I’ll begin discussing some of the nasty techniques used for identity theft and how to defend oneself against them.

Stealing physical credit cards and creating fake ones are part of the criminal technique called “carding.” One of the significant recent successful investigations and prosecutions of an international credit-card fraud ring began with the US Secret Services’s Operation Firewall in late 2004. The investigators discovered a network of over 4,000 members communicating through the Internet and conspiring to use phishing, spamming, forged identity documents (e.g., fake driver’s licenses), creation of fake plastic credit cards, resale of gift cards bought with fake credit cards, fencing of stolen goods via eBay, and interstate or international funds transfers using electronic money such as E-Gold and Web Money.

In October 2004, the Department of Justice (DOJ) indicted 19 of the leaders of Shadowcrew;<http://www.usdoj.gov/criminal/cybercrime/mantovaniIndict.htm> by November 2005, 12 of these people had already pleaded guilty to charges of conspiracy and trafficking in stolen credit card numbers with losses of more than $4M.<http://www.usdoj.gov/criminal/cybercrime/mantovaniPlea.htm>

In February 2006, Shadowcrew leader Kenneth J. Flury, 41, of Cleveland OH was sentenced to 32 months in prison with 3 years of supervised release and $300K in restitution to Citibank.<http://www.usdoj.gov/criminal/cybercrime/flurySent.htm> In June 2006, co-founder Andrew Mantovani, 24, of Scottsdale AZ was fined $5K and also received 32 months of prison with 3 years of supervised release. Five other indicted Shadowcrew criminals were sentenced with him. By that time, a total of 18 of 28 indicted suspects had already pleaded guilty.<http://www.usdoj.gov/usao/nj/press/files/mant0629_r.htm>

One of the lessons we teach our “CJ341 Cyberlaw & Cybercrime” students at Norwich University is that everyone with a credit card ought to check their statement immediately upon receiving it. Every line should be recognizable; if it is not, call your credit-card company to find out what a particular charge is for and where it was charged. Tell your company to freeze your card account if there is any question of its having been compromised. Write down the details of every conversation with the credit-card company employees (date, time, name of employee, case number) in case you need evidence to clear your own name. Contact the three major credit-reporting agencies (Equifax<http://www.equifax.com/>, Experian<http://www.experian.com/>, and TransUnion<http://www.transunion.com/>) to tell them to freeze your credit report to make it harder for criminals to apply for loans or open bank accounts in your name until you release your credit records when _you_ want to, not when the criminals want to.

Another tool is to ask for your free annual credit report on yourself from each of the three credit-reporting agencies using the official AnnualCreditReport site.<https://www.annualcreditreport.com> You may want to ask for one report every four months by
spacing out your requests to the three agencies so that you can spot unexpected changes (e.g., a request for a car loan in a state 3,000 miles from your home) more quickly than if you order all three at once. The AnnualCreditReport.com site mentioned above also provides extensive information in its Frequently Asked Questions <https://www.annualcreditreport.com/cra/helpfaq> that will help consumers interact effectively with the agencies.

* * *

I hope that you will find this information useful for yourselves and for your colleagues and employees. I remind readers that I own the copyright to all my Network World articles and that my colleagues at Network World and I are delighted if you choose to use them verbatim in your internal security newsletters. There is no charge and you do not have to ask us for permission. However, if you do use these articles, please have the courtesy to include a pointer to the URL of the article in the Network World Security Strategies archive.

* * *

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance <http://www.graduate.norwich.edu/infoassurance/> and CTO of the School of Graduate Studies at Norwich University in Northfield, VT. Mich can be reached by e-mail at <mailto:mekabay@gmail.com>; Web site at <http://www.mekabay.com/index.htm>.

Copyright © 2008 M. E. Kabay. All rights reserved.

Permission is hereby granted to Network World to distribute this article at will, to post it without limit on any Web site, and to republish it in any way they see fit.