Secrets of a former credit card thief

http://www.creditcards.com/credit-card-news/secrets-former-credit-card-thief-dan-defilippi-1282.php

January 14, 2011

Card theft is cheap, easy and you could be next

By Michelle Crouch

We've all heard the standard tips about preventing identity theft and credit card fraud. But what would a real identity thief tell you if he had the chance? Dan DeFelippi, who was convicted of credit card fraud and ID theft in 2004, says simply this: You can't be too careful.

DeFelippi, 29, mostly made fake credit cards with real credit card information he bought online. "I would make fake IDs to go with them, and then I'd buy laptops or other expensive items in the store and sell them on eBay," he says. DeFelippi was also involved in several other kinds of scams, including phishing schemes that exploited AOL and PayPal customers. Committing credit card fraud is still "ridiculously easy to do," he says. "Anyone with a computer and $100 could start making money tomorrow."

Dan DeFelippi

After his conviction, DeFelippi faced eight years in prison, but under a plea deal he agreed to community service and to pay back more than $200,000 in restitution. He also worked for the U.S. Secret Service, helping to infiltrate the online underground and training agents in the latest fraud techniques. His help led to the arrests of five to 15 people over two years. Today, he's a Web developer at a graphic design company in Rochester, N.Y. He agreed to take an hour with CreditCards.com to share his story and his top tips on how to protect yourself.

CreditCards.com: How did you get started?
Dan DeFilippi: When I was in middle school and high school, I was into what I would call innocent hacking. I wasn't trying to be malicious or make money. I was just interested to see what I could do. In college, I started selling fake IDs to make a little extra money. I was pretty active in online chat rooms where people would talk about this stuff, and I began to realize there was a whole world of credit card fraud where I could make a lot of money with very little effort. From there, it was just a huge downward spiral.

CreditCards.com: You said you bought credit card data online. Tell me about

that.
DeFilippi: Every credit card has magnetic stripe on the back with data on it. There are people out there who hack into computers where that data is being stored. There are also people like waitresses and waiters with handheld skimmers who steal the data that way. Then they sell the data online. I'd pay $10 to $50 for the information from one card. Then I'd use an encoder to put that data on a fake card, go into a store and purchase stuff.

CreditCards.com: Do identity thieves like some credit cards better than others?
DeFilippi: Well, a lot of American Express cards have no set limit, so you'd be able to buy a lot more. However, the downside is that a lot of merchants require more security for American Express than for other cards. They may ask you to enter the four-digit code on the front of the card or your ZIP code. That information usually isn't in the magnetic stripe information. So if a card is skimmed, if someone has its magnetic stripe information, they would still need the number on the front or your ZIP code to commit fraud.

CreditCards.com: What about debit cards?
DeFilippi: I always recommend against them. With debit cards, it's your real money in your bank account you're playing with. So if someone gets your debit card information and uses it, your cash is gone until you fill out a lot of paperwork and persuade the bank to give it back to you. Credit cards are much better at protecting you against fraud. And if you're worried about debt, you can always pay them off every month.

CreditCards.com: What's your No. 1 tip on how consumers can protect themselves?
DeFilippi: You've probably heard this before, but the most important thing really is to watch your accounts. And I don't mean just checking your statement once a month. If you're only checking your statement once a month, someone can start using your card at the beginning of the billing cycle, and they can do a lot of damage before you catch it. You're talking thousands of dollars, and it will be a lot harder to catch them and dispute it. I use Mint.com, which is a free aggregation service that allows you to put all your accounts on there and monitor everything at once. I check that every day. It's also a good idea to check your credit report at least twice a year to make sure no one has stolen your identity.

If you're only checking your statement once a month, someone can start using your card at the beginning of the billing cycle, and they can do a lot of damage before you catch it.

CreditCards.com: Is online shopping safe?
DeFilippi: You've got to be careful. It is really easy to create a fake online store or to create a store that sells stuff, but its real purpose is to collect credit card information. I'd try to stick to reputable sites or at least to sites that have reviews. A lot of times they'll create these stores that sell things that are widely searched for at prices that are incredibly low. If a deal is way too good to be true, it's probably a scam and they just want your information. The more information a website asks for, the more you need to be certain that

this is information they really need and it's a legitimate site. Also, don't buy anything from somebody e-mailing you, no matter how good the offer sounds. If a company is sending you an ad through e-mail and you've never heard of the company, don't buy anything from them.

CreditCards.com: How did your phishing scams work?
DeFilippi: People are much savvier now. Back when I started, it wasn't that common. I was getting thousands and thousands of responses from single mailings. The first one I did, I targeted AOL users, because I thought they would be less computer literate and more likely to fall for my scams. We said, "Your credit card information has expired. Come to this site and update your information or your account will be closed." I did something similar with PayPal. I sent an e-mail that said, "Someone has accessed your account. We've locked your account. Please click here to access your account." We'd link them to a fake website and they'd give us their PayPal log-in information. Then we'd say, "For security purposes we've removed your account information. Please re-enter it."

If you're using an open Wi-Fi connection you should pretty much have the expectation that there is no security.

CreditCards.com: Where did you get the e-mail addresses for your phishing schemes?
DeFilippi: There's software that allows you to harvest them from anyone who has posted their e-mail addresses online, so don't ever put your e-mail address on a website. If I was targeting a specific group, I'd try to find e-mails for that group. For the PayPal scam, I was trying to find people around my age or younger, so I targeted college and universities. I looked for ones in Massachusetts because I could make fake IDs from Massachusetts. As part of the scam, I'd get their date of birth, address, Social Security number and driver's license number. Then I could make a fake ID that had all accurate information on it. The only thing that wouldn't be real would be my picture. It's kind of scary how much information I could get.

CreditCards.com: What other mistakes do consumers make on the Web?
DeFilippi: When you're using your computer online, it's sending data back and forth between your computer and website. If someone gains access to that connection -- it's called sniffing -- they can capture the data between you and the website you're communicating with. That's the reason it's so important to access secure websites if you're putting in any sensitive data, so look for "https" in the Web address. A more recent issue is the free wireless offered all over the place. If you're using an open Wi-Fi connection, you should pretty much have the expectation that there is no security.

CreditCards.com: What steps do you take to protect your own data online?
DeFilippi: All financial services companies have two-factor authentication. So you typically have to put in a password plus something else. A lot of banks use questions, but that can actually give you a false sense of security because you can find out a lot of information about people online. So maybe this is extreme, but for those questions, I make up stuff. I don't put in my real information. For example, a common question is: "What city

were you married in?" Well, I'm not married, but I'll answer that question so there's no way anyone could possibly know the answer. I try to make sure at least one of the questions has a made-up answer.

CreditCards.com: What's your advice on using ATMs?
DeFilippi: ATM skimming is the big thing right now because it's cash, and cash is king. Basically, that's where someone puts a card reader on the ATM machine, captures your PIN, then goes and drains your bank account. The skimmer device goes over the card slot, and it's designed to look like part of the ATM. Some of the equipment now is very good and it's hard to tell the difference between that and a real machine. So what you need to do is try to use the same ATM every time, and watch out for anything on the machine that looks out of the ordinary, especially something stuck on the front where you put your card in. Generally, I like to use ATM machines at banks rather than convenience stores or a bar or club. There have been incidents where thieves installed their own ATM machines in places with skimmers inside them. That's much less likely to happen at a bank.

CreditCards.com: Is there more the banking industry could do to protect us?
DeFilippi: The biggest thing they could do is get away from using magnetic stripes. They aren't that secure and anyone can get a magnetic stripe reader (a skimmer) for $5 to $10. The smart chips that are widely used in Europe and internationally are much more secure and harder to hack. They offer near 100 percent protection against fraud, at least from a skimming point of view, and they also require a PIN. But the credit card companies have done the math. They think people will use their credit cards less often if they had to put in a PIN. It might eliminate a lot of the fraud, but there would be less card use and they would end up losing money. So they're actually doing just the opposite, moving to a system where you can just have your credit card in your pocket -- you don't even have to swipe it to use it. The problem is, that's very unsecure. Anyone with equipment can sit out in their car and pick that up.

CreditCards.com: How did you end up getting caught?
DeFilippi: I went to Best Buy with a guy I was working with locally to buy a laptop, and the manager there was pretty well trained. When he swiped the card, he asked for my friend's ID. Most stores don't ask for ID. My friend gave him his fake driver's license, but then when the manager swiped the credit card, it came up "Call for authorization." A call for authorization, if you're trying to commit credit card fraud, is really bad; it means the credit card company has seen suspicious activity. The manager said he needed to go to the front desk to finish processing the order. As soon as he left, we walked as quickly as possible to the exit and left the store. The problem was, my friend had given the manager his fake ID with his picture. They ran it on the news and caught him. He told them the whole story, so they ended up catching me, too. I really was better off getting caught when I did. I was lucky I didn't go to prison. Under the guidelines now, I'd probably have to serve at least two years. So anything I can do to help people now, to help compensate for what I've done, I'm trying to do.

See related: How to check for, fix, ID theft or fraud, Anatomy of a credit card, When hit by ID theft, take these 4 steps to make things right, How to check for, fix, ID theft or fraud, U.S. credit cards becoming outdated, less usable abroad

Published: January 6, 2011

Three most recent Legal, regulatory, privacy issues stories:

SHARE THIS

<a href="http://www.

SHARE

FOLLOW US