



You Asked, We Answered: An Identity Theft Expert Tells All

An Industry Insider Answered Viewers' Questions About I.D. Theft

May 2, 2008—

We submitted some of your questions to Dan Clements, an identity theft expert and founder of CardCops.com, a division of the Affinion Group. He was one of the pioneers in finding compromised data in cyberspace and figuring out how to return it to consumers and banks in real time. He has designed "stings" to capture data and intelligence, which have also provided behavior on hackers. He is frequently quoted in national and global news outlets, and he lends his expertise to law enforcement.

We have also submitted some of your questions to a U.S. Secret Service agent and will post those answers later this week on ABCNEWS.com.

Rob from Erie, Pa., asked: "How do I know if I am a target for identity theft????"

Clements answered:

You really don't know until it's confirmed with some type of action. But you can look for signs, like your accounts getting hit with \$1 charges. Thieves sometimes use donation sites like the Red Cross to validate a card or debit account.

Annie from Redondo Beach, Calif., asked:

"Every credit card company tries to sell you fraud protection at approx. \$8 per month. Is it worth the money?"

Clements answered:

If it's a service from the credit bureaus, it is worth it because you can see "inquiries" and newly opened accounts in your name. If you don't recognize what's on your credit files, you should investigate. Other services can tell you pre-emptively that your personal information may have been breached.

Dave from Bakersville, N.C., asked: "Sir; just how do you protect yourself from ID theft? I use equifax to help guard me, is that good enough?"

Clements answered:

Always watch your online accounts like a hawk. A simple \$1 charge could be the thieves' pinging your account for validity. Get a new credit card number on its anniversary, re-PIN any debits cards every six months, and pick up a shredder.

Shirley from Brooklyn, N.Y., asked:

"My home computer has been infected with a virus called "Spyware or Spywave." From what I understand it is like someone is watching me. Have hackers find a way to look into all the websites I have visited with my info (such American Express, Fidelity investments, and online purchases). I

have subscribed to all three credit bureaus for quarterly reports and paid extra on some of my credit cards for fraud. What more could I do to protect myself?" **Clements answered:**

Have a technician clean your hard drive or reformat it to rid the virus. Don't download any program from any unfamiliar site. Always type the actual web site into the browser window, don't copy and paste. Never click on a link in an email. Lastly, make sure your financial accounts are all at an https address, the "s" means secure.

Martha from Peabody, Mass., asked:

Is there any way for me to know if my information has been breached before someone actually sells it or uses it?

Clements answered:

Yes, a service called ID Secure.com from the Affinion Group tells you if they find your personal information out in cyberspace. They scour chat rooms, Web sites and message board forums to try to locate your data. If they find your debit or credit card, e-mail or Social Security number, they will notify you in real time.

Lois from Downingtown, Pa., asked: "Will a firewall and Internet security software prevent thieves from accessing credit card information online?"

Clements answered:

It helps, but the thieves really have infinite ways to get into the e-merchants servers. Visa estimates only half of their online merchants meet their security requirements. But consumers have limited liability for credit cards and debit cards if they react and notify banks in a reasonable period of time.

Mr. McQ from Lynchburg, Va., asked:

Which way would you suggest to have your credit report? Internet, phone, or mail, since your SOC. Sec. number is mandatory for this process to take place. Thanks for your help.

Clements answered:

Any of the above, since the credit bureaus are supposed to truncate your Social Security number and any listed account numbers.

Randy & Angela from Winfield, Kans., asked:

"In the last two weeks we have had someone e-check our account for \$19.95 & 19.75. We want to know if they are fishing our account to see if we will notice to maybe try a larger amount? We've had both of these amounts removed through our bank but are concerned were are they coming from & if at all if we can stop them?"

Clements answered: Notify your bank. Worst case scenerio is you may have to close that account.

Gabriel from Rosharon, Texas, asked:

"My identety was stolen two weeks ago, now, I have several CC open, and charged I contacted all the creditt buruos and the police, what do I do next"

Clements answered:

Get a police report and fill out all the necessary affidavits with your bank. Then put a "fraud alert" on all your credit files. Creditors will now have to call you to open new accounts.

Copyright © 2008 ABC News Internet Ventures