What happens when you swipe your card?

As hacking of top retailers make headlines, Bill Whitaker discovers how insecure your credit card information is this holiday season

The following is a script of "Swiping you Card" which aired on Nov. 30, 2014. Bill Whitaker is the correspondent. David Schneider, producer.

This holiday shopping season you might worry that every time you swipe your credit or debit card some criminal might be swiping your account number and with good reason. The number of reported, illegal intrusions into the computer systems of U.S. companies is at a record high this year and climbing. The hacking of Target, Home Depot, Staples and other top retailers made headlines. Behind the headlines are two separate crimes with two sets of criminals. Sophisticated cyberthieves steal your credit card information. Common criminals buy it and go on shopping sprees -- racking up billions of dollars in fraudulent purchases. The cost of the fraud is calculated into the price of every item you buy. When computer crooks swipe your card number, we all end up paying the price.

2014 is becoming known as the "year of the data breach." The theft of 40 million credit cards from Target late last year was followed by news of a breach at Michaels stores involving more than two million credit cards. Then came P.F. Chang's. And in September, Home Depot announced that 56 million of its customers' credit card numbers were stolen.

Dave DeWalt: Nearly every company is vulnerable.

Dave DeWalt is CEO of FireEye, a cybersecurity company that gets hired to keep hackers from getting into a company's network or getting them out after there's been a breach.

Dave DeWalt: Even the strongest banks in the world-- banks like JPMorgan, retailers like Home Depot, retailers like Target -- can't spend enough money or hire enough people to solve this problem.

Bill Whitaker: Cybersecurity is a misnomer? There is no cybersecurity it sounds like you're saying.

Dave DeWalt: This isn't a lack of effort. Most of the large companies are growing their security spend. Yet 97 percent -- literally 97 percent of all companies -- are getting breached. So there's a gap here.

Bill Whitaker: Ninety-seven percent?

Dave DeWalt: Ninety-seven percent. In fact, we...

Bill Whitaker: That's outrageous.

Dave DeWalt: It is outrageous. It's pretty amazing.

FireEye tracks assaults on its clients with a real time map showing where computer attacks originate and their targets. It's an eerie throwback to Cold War illustrations of what a nuclear missile attack might look like, but with cyber attacks...

Bill Whitaker: This goes on 24 hours a day.

Charles Carmakal: 24 hours a day, yeah.

Charles Carmakal leads teams of first responders for FireEye.

Charles Carmakal: We are seeing hundreds of thousands of attacks on a weekly basis across the globe.

Bill Whitaker: And these are just the ones that your systems are picking up.

Charles Carmakal: That's right.

Dave DeWalt: On average the breaches from the time of infection, from when the bad guys get in to the time they are discovered, is a whopping 229 days. 229 days.

Forensic investigations reveal that 80 percent of security breaches involve stolen and weak passwords. One of the most common is: 123456.

Dave DeWalt: The days when we have our username and password, which is our son or daughter's name or our cat or our dog is not enough security for, you know, for today's attackers. Breaches are inevitable. It's happening. It's just life that we live in today.

Bill Whitaker: Inevitable?

Dave DeWalt: Inevitable.

Bill Whitaker: Just accept that...

Dave DeWalt: Accept that a little bit...

Bill Whitaker: ...they are going to get in.

Dave DeWalt: They're going to get in. But don't let them access the information that's really important. Don't let them get back out with that information. Detect it sooner. Respond sooner. And ultimately that exposure is very small. Maybe they got away with a few credit cards. Maybe they didn't get away with any credit cards. But they didn't steal 56 million of them or 40 million of them.

"You know, they're running a business. And frankly they're not focused on cybersecurity."

Target declined our request for an on-camera interview, but the breach of its security a year ago is a case study in how hackers operate. It started when criminals stole the username and password from one of Target's vendors -- a Pennsylvania heating and air conditioning company. The credentials got them into Target's network without attracting attention. Once inside they easily spread to thousands of checkout terminals in nearly every store. The hackers then installed malicious software, or malware, to record card swipes.

Dave DeWalt: The company invested a lot of money in security. It wasn't like they weren't trying to stop the bad guys. It's just the bad guys were really good, number one. Number two, they're very persistent.

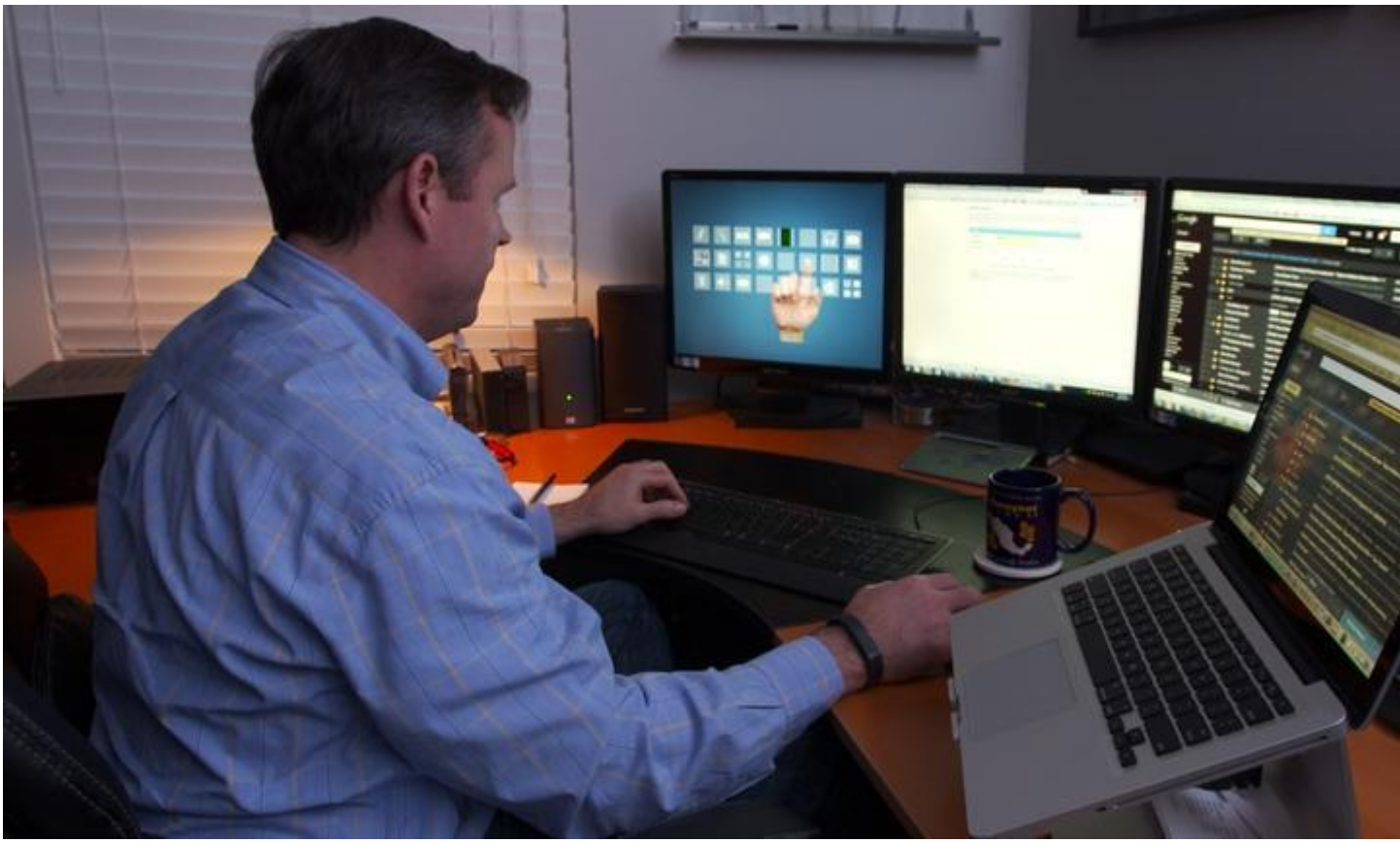
A security system Target recently bought from Dave DeWalt's company, did detect the intrusion, and triggered alarms. But Target's older security systems were still in place, generating millions of alerts similar to these. Most were for minor technical glitches and the warnings from FireEye were lost in the noise.

Bill Whitaker: So alarms were going off?

Dave DeWalt: Alarms were going off. And when you get millions of alerts a day and there's one or two alerts that are the ones blinking red, "There's a problem. There's a problem." You can miss it and it's very hard to find the needle in the haystack. So Target's problem ultimately became, "I couldn't find the needle. I couldn't see the one alert that was bright red."

Last December 18, a week before Christmas, a cybersecurity blogger named Brian Krebs first reported the story publicly.

Brian Krebs: The breach lasted for a little more than three weeks. But they actually managed to hit Target at the busiest time of year for them.



Krebs' office is like a computerized crow's nest: a high-tech perch from which he scours the cyberworld for early signs of underworld activity. Over the past year he broke the news on his blog that criminals had hacked into a dozen retailers and chain restaurants including Dairy Queen and The Home Depot.

Brian Krebs: A lot of times those companies have already been notified by law enforcement, by Secret Service or the FBI.

Bill Whitaker: But it sounds like it's usually discovered by people outside of the company.

Brian Krebs: That's almost universally true. Yes.

Bill Whitaker: Why is that?

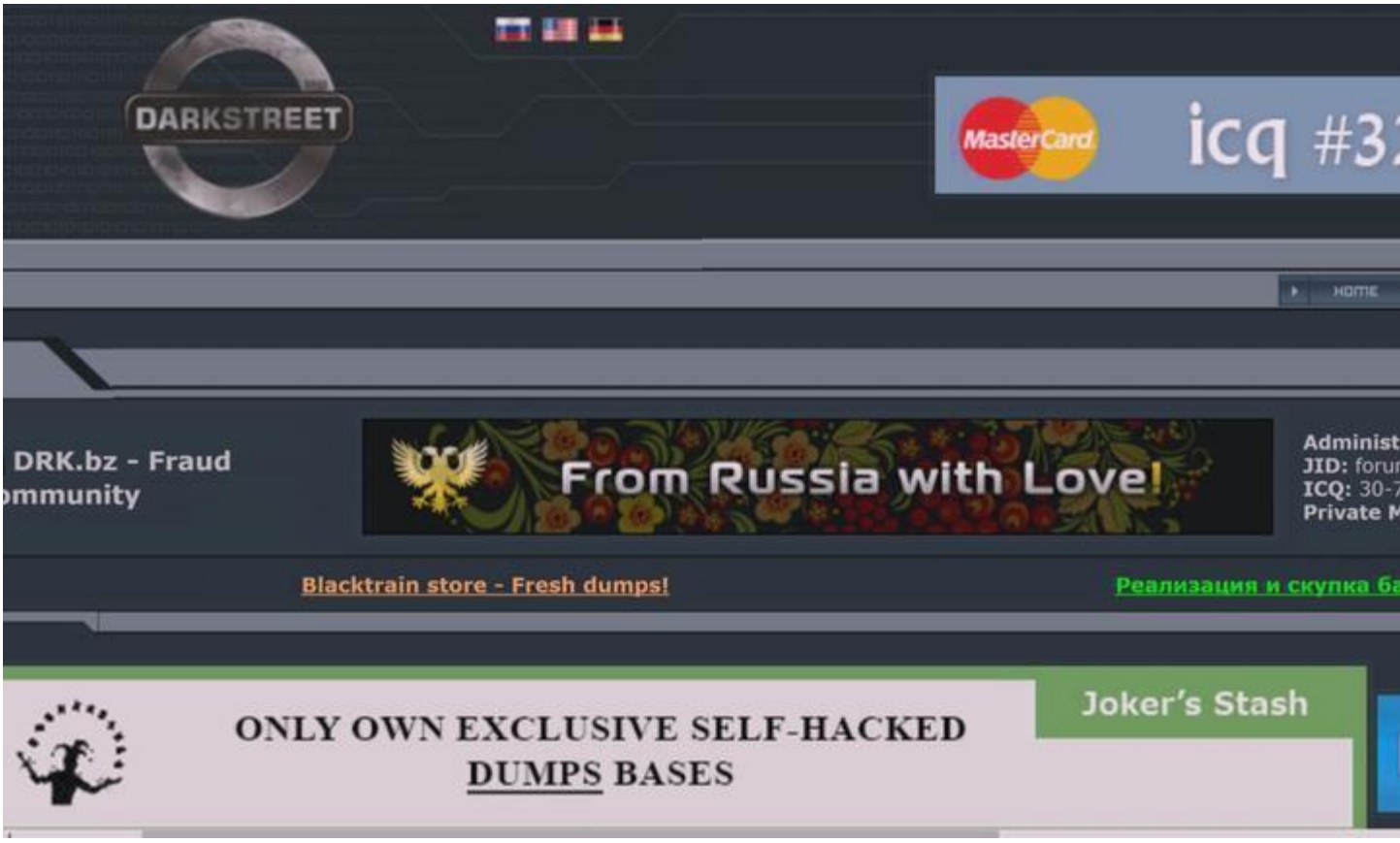
Brian Krebs: A lot of times the first indicators that you get that one of these organizations is comprised is when their customers' financial information goes up for sale in the underground. You know, they're running a business. And frankly they're not focused on cybersecurity.

There are scores of sinister online shopping bazaars where cyberthieves put their goods up for sale. Think Amazon.com for thieves. This is where Krebs does his detective work.

Bill Whitaker: They're just right on the Web? You can buy stolen cards by just going to this site?

Brian Krebs: Absolutely.

Big batches of stolen card numbers are called dumps. Krebs figures out which banks have customers' stolen cards up for sale and alerts them. The banks then check to see which merchant is the common link.



Brian Krebs: If they're willing to share that information with me, I can take that and go back to other banks and say, "Look, this is the pattern they're seeing. What are you seeing?"

The bulk of cards sell for anywhere from 10 to 50 dollars, depending on things like the expiration date, or the credit limit.

Brian Krebs: In the case of Target they stole 40 million cards. But you know how many cards they managed to sell? About five percent of those.

Bill Whitaker: That's still a lot of cards.

Brian Krebs: It's still a lot. And I say "only" because each of those cards, the average price was about 20 dollars per card. So that's a lot of money any way you slice it.

"The banks are the victims who are actually paying for the breaches, rather than the retailers..."

The thieves offer volume discounts and sales and customer service includes refunds if the cards have been cancelled.

Brian Krebs: If you buy from them and it comes back as declined, they'll automatically credit the amount that you bought for that card cost. So they'll automatically credit your account.

Bill Whitaker: You're kidding. This stolen card will work or you'll get your money back?

Brian Krebs: Yeah, absolutely.

Customers are told to make payments with Western Union or other money transfer methods. Credit cards are not accepted. The masterminds behind the hacking and selling of stolen card data are sophisticated crime syndicates. Most are in Russia and Eastern Europe -- primarily Ukraine -- and out of the easy reach of American law enforcement. Ed Lowery heads the criminal division of the U.S. Secret Service, which investigates financial cybercrimes.

Bill Whitaker: The fairly big breaches we've been seeing -- Target, Home Depot. Who's behind that?

Ed Lowery: Well, those are professional cybercriminals. Those individuals, they make their living -- and a very good living, at times -- attacking the U.S. financial infrastructure. That level of cybercriminal. That is the new-age cartel, as it were.

Secret Service arrests have led to the convictions of 14 people, but there are plenty of others to take their places. The criminals buying the stolen numbers don't have to be that sophisticated.

Bill Whitaker: Is it fairly easy to turn those numbers you buy online into one of these cards?

Ed Lowery: Now, I really don't want the general public to think that they should go out and start committing fraud. But obviously, the encoding and all takes a little higher level of sophistication. And you have to have the criminal drive to do it. But is it highly technical? In light of the intrusions we're speaking about, and the rest, it's not nearly that sophisticated.

Buyers are all over the world. In the U.S., street gangs are among the crooks to use stolen cards. They buy gift cards, which are like cash, and electronics, which they resell for quick profits.

Brian Krebs: If you buy a card for 20 bucks and you can make 400 dollars off each card, that's a pretty good return on your investment.

Bill Whitaker: Pretty good.

For many banks, news of a breach from Brian Krebs is the first sign they have of a problem. Two of his regular readers are Barry Abramowitz, chief information officer for Liberty Bank in Connecticut, and Linda Swartz, who heads up security for Westfield Bank in Massachusetts.

Bill Whitaker: So you don't hear about it until Brian Krebs breaks it?

Linda Swartz: Pretty much.

Barry Abramowitz: That's what makes his work so valuable.

Linda Swartz: Exactly. If you know there's a problem, you can stop it from occurring or stop the bleeding before it gets too bad. But you need to know that information.

Most banks and credit unions rely on MasterCard, Visa and other card companies to notify them when a customers' account may have been stolen, but they're not told which retailer was hacked or when.

Bill Whitaker: Why don't they tell you which retailer is responsible or involved?

Barry Abramowitz: I don't know.

Linda Swartz: Probably so it doesn't place the blame on the merchant who was compromised. They don't want us to go back to that merchant and say, "You know, your system was compromised. You lost my customers' information."

Bill Whitaker: Why not?

Linda Swartz: It's business. I mean, I hate actually saying that it was Home Depot and Target, but those are the ones that are in the media.

"The cards themselves are fundamentally fraud-prone."

Bill Whitaker: How big a problem are these security breaches for the banks?

Barry Abramowitz: Huge.

Linda Swartz: Yeah.

Barry Abramowitz: Huge.

In 2013, stolen credit cards led to estimates as high as 11 billion dollars in fraud in the U.S. That doesn't include the cost to banks of replacing millions of cards and monitoring customers' accounts for suspicious activity.

Bill Whitaker: So when the customer is told that he's not going to lose anything out of his pocket. The customers not going to pay for the fraud, somebody's paying for it.

Linda Swartz: The bank.

Barry Abramowitz: The banks are the victims who are actually paying for the breaches, rather than the retailers that have had the information compromised.

The Home Depot, like other recently breached retailers, declined our request for an on-camera interview, citing ongoing investigations. Mallory Duncan is with the National Retail Federation, the industry's largest trade group. He says the magnetic stripe cards are just too easy to counterfeit.

Mallory Duncan: The underlying problem is that we have cards that were designed for the 1960s, '70s and '80s but we now have hackers who are using 21st century tools to break in.

Bill Whitaker: Are the retailers really doing everything they can to secure customers' information?

Mallory Duncan: We're doing everything we possibly can to secure it.

Bill Whitaker: What does that mean "possibly can"?

Mallory Duncan: Well, because the problem is you're trying to secure a house of straw. The cards themselves are fundamentally fraud-prone.

After a year of relentless breaches, bankers, retailers and security companies all agree the technology behind credit cards is broken and needs to change. Visa and MasterCard declined to be interviewed, but said the roll out of credit cards with computer chip technology next year will make counterfeiting cards almost impossible.

Bill Whitaker: Apple and Google are promoting their own payment systems to protect account information and retailers, like The Home Depot, are encrypting the data. The changes will cost billions of dollars and take years to implement.

Bill Whitaker: This Christmas shopping season, you're expecting this to happen again.

Linda Swartz: Absolutely. We know it's going to. It's inevitable. We feel like we're just kind of sitting and waiting for it to happen. There's not a lot we can do to stop it.