TRAINING AN EFFICIENT DRAW | STASH IN CACHES | HOW CREDIT CARDS ARE EXPLOITED

TACTICS AND PREPAREDNESS

SKILLS AND

OCTOBER 2014 ISSUE 12 - TACTICSANDPREPAREDNESS.COM

SELECTING A 4X4 ANYWHERE IN THE WORLD

BY: GLEN EDMUNDS | PHOTOS BY GLEN EDMUNDS (WWW.GLENEDMUNDS.COM)

If you are about to be deployed into a region where you will be required to drive or purchase a used four wheel drive (4WD) vehicle or simply holiday in remote areas, the following information could help.

It's not easy finding the car for your needs and often you run up against the used car salesman who would sell his grandma for profit. It doesn't matter where you are in the world, it's always important to know a thing or two about what you're looking for before you hand out your (or your company's) hard earned cash.

Good second hand 4WD vehicles can be obtained everywhere and are readily available at a cost. If you're in the USA the cheapest second hand models may be American models, but if you're about to ship out to another region you would do well to think about a Japanese vehicle that would be much more reliable, affordable, easy to maintain and have readily available spares.

In most cases, every good second hand car is going to be expensive. Finding the correct one can be time consuming, laborious and frustrating, but stick with it. The old adage, "there's someone for everyone out there," works the same for when buying used vehicles, but you've got to be patient.

WHAT TO LOOK FOR

Finding the right vehicle is crucial, so here are a few tips on what to look for while scouting around:

Test drive the car—hard. Ensure it goes into 4WD easily and there are no strange noises. If you're going to use it off road, then test it off road.

If you can, get it checked by a reliable, trustworthy source. Get it on a hoist, so you can check underneath and see if it's had a hard life or not.

Ensure the paper work is in order. Don't hand over any money until you're sure.

Once you choose the vehicle, take some photos and note the extras and the tires. You will want to ensure they are still the same when the vehicle is delivered.

Choose the right vehicle for your needs. If you are going to do a lot of

continued on next page

HOW CREDIT CARDS ARE EXPLOITED BY CRIMINALS

BY: DR. BRANDEN R. WILLIAMS

IMAGE BY SHUJENCHANG

An EMV card.

IMAGE BY ASIM18

A Chip Authentication Program (CAP) card reader used in conjunction with EMV cards.

Another day, another credit card breach.

Another envelope headed to your house with a new card. Another hour wasted adding new payment information into your suppliers or utilities that use auto-pay. It seems that this is the new routine in 2014 as we have seen major breaches from banks, government institutions and retailers alike. There is a security standard designed to protect payment card data, but it is obviously not having the desired effect of keeping this data safe.

If you take out your wallet right now, I am willing to bet there are at least three payment cards in there (if not many more) with either a Visa, MasterCard, American Express or Discover logo on it. One is probably tied to your checking account and doubles as a debit card, the others are credit cards with some kind of limit on them. I'm also willing to bet that the amount of cash you use and carry is less than it was ten years ago. Cashless payments have made it easier for us to part with our money—and in higher amounts. Research shows that merchants who accept payment cards will see higher average ticket sizes on checkout as well as more sales of big ticket items. As the cost to process these transactions decreases, it helps speed along smaller payments too. Swiping or waving a card for a purchase of less than $25 doesn't require a signature (in most cases), so you get through faster and the merchant carries less cash.

International travelers know that cards inside the U.S. are missing something that cards issued in most of Europe, Canada and parts of the Asia-Pacific part of the world have. Those countries use cards that have a chip in them, which increases the security for card-present transactions. That is, when you pay for something by physically presenting the card and not online. Technically called EMV, but sometimes referred to as Chip & PIN, this twenty year old technology leverages similar encryption techniques to those used to protect your PIN from a debit transaction. Even though it is old technology, it reduced card-present counterfeiting fraud dramatically in countries where it is deployed. Retail companies point to EMV as the grand solution to payment card security, but they are wrong. Chances are, the breaches still would have happened even with EMV cards.

Your next replacement or newly issued credit card will, most likely, have one of these chips in it and some of your cards may already have one. Apple's announcement for integrating payments into their ecosystem via Apple Pay will surely add to the complexity (and potentially, the security) of payments as well. We need more security in the payment systems here in the U.S. as magstripe technology is really at the end of its usable lifespan. The concept behind these new chip cards is to replace the static data in the magstripe with dynamic crypto codes inside the chip to authenticate the card. As an example, if you go to your nearest Walmart and present a chip card for

payment, you must use the chip reader. Swiping the card will not work. This means that if someone steals the static magstripe off of the card and presents it at a terminal that has an active EMV slot, it won't work. This is a huge advantage and will cut down counterfeit cards dramatically, until the bad guys figure out a way around EMV's technology.

We need EMV because credit cards in the U.S. are particularly vulnerable to a type of attack called "skimming." For about $25 an attacker can purchase a device that allows them to read the data inside the magstripe of your card and clone it to another card. In this case, the attacker must have possession of your card as they would when you paid for a meal at a restaurant or any other time that your card is out of your sight. I am not, however, recommending you change your behavior around the treatment of your card, for reasons I will reveal momentarily.

It's pretty easy to skim a card physically, but with higher risk as you are interacting with the victim. Another kind of skimming is through devices that are placed inside or on top of existing card readers. If you turn to your nearest search engine and look for "ATM skimmers," you will figure out just how creative these guys are getting. Not only are they able to miniaturize components and leverage technologies like Bluetooth and WiFi to communicate with skimmers once they are installed, they also have access to injection molding machines that make realistic parts to sit on top of the card reader. In some cases, it's nearly impossible to tell whether an ATM or a payment terminal has a skimmer in it without tedious inspection. The bad guys are getting really good, but many of the controls we pursue today begin to remove some of their ability to scale—forcing physical interaction with the devices to compromise them. Any time you require the physical touch of something to compromise it, Locard's exchange principle states that a criminal will both bring something to, and take something away from, the crime scene. The fear of leaving physical evidence that leads law enforcement to your door is a good deterrent for white-collar criminals.

I mentioned that criminals are getting better at miniaturizing their equipment, which allows for some interesting types of attacks. In particular, there is a whole new area of research that uses something called a side-channel attack to capture sensitive information like a PIN. An example of this type of attack is using the accelerometer in an iPhone sitting on someone's desk to detect key presses on a keyboard. Because these devices are extremely sensitive, researchers have demonstrated in lab environments the ability to use sensing equipment commonly found in popular smartphones to capture information such as a password on a keyboard. It's called a side-channel attack because the keyboard was not compromised, but normal usage leaks information into the environment through other methods.

Humans are notorious for leaving trails of themselves in their environment. An example of Locard's exchange principle in a non-criminal operation is using your fingers to press down keys that enter a PIN into a terminal for a Debit transaction. Depending on the type of keyboard, you will transfer heat from your fingers onto the keys which an infrared camera can detect. In true miniature fashion, you can now purchase infrared camera attachments for your iPhone for the same price as their new watch. The attack is remarkably effective and the residual heat is detectable for at least a minute after the PIN entry.

All is not lost, however. We live in a world of ever changing risk and we all just need adequate tools to happily survive and exist. Payment card technology is outdated and generally flawed from a security perspective, but there are things coming that may change how we view payments both as consumers and as proprietors of our own businesses. I want to leave you with some tips that you can follow that will greatly reduce your risk of falling victim to credit card fraud. Remember, though, even if you do, as long as you pay attention to the transactions hitting your accounts you will only suffer the headache of switching out the card itself (including in all of your auto bill pay services.)

WHAT CAN YOU DO?

Even though the attacks are more creative and using better technology in recent years, there are still things we can do to protect ourselves. Fundamentally, as a consumer, you are better off not carrying cash and instead sticking with payment cards. If someone steals your wallet and it is full of cash, you won't be getting that back. But thanks to some limits on consumer liability, vigilance on your part will keep your electronic cash in your pocket. The basic rules are that credit card fraud carries zero liability and debit card fraud can carry up to $50 of liability if you report fraud in a timely manner. Many banks will give you zero liability on debit card fraud as well, as long as you report

Memorizing and scratching off the CVV code on your card can help eliminate some forms of card theft.

it quickly. Here are a few tips that can keep you safe:

Credit transactions (no PIN) can be safer than debit transactions (with PIN). I always advise my family to sign, never enter a PIN.

If you must use a PIN (such as at an ATM), make sure the PIN-entry device is in a well-lit area, does not appear to have loose wires or stickers peeling off and has intact tamper-proof tape.

In addition, cover the keypad when entering your pin and be sure to touch all of the numbers so that you transfer an equal amount of heat to prevent someone from stealing your PIN via an infrared side-channel attack.

Most importantly, *be vigilant about keeping up with every transaction.* Set up alerts on your payment card and banking websites so you know when transactions over a certain amount occur. If you see something, say something!

ADDITIONAL READING:

Do you want to see the video of how you leave infrared trails behind you? Check out http://brando.ws/irpins14 to see how it works.

Dr. Edmond Locard is considered the father of modern day forensic science. Learn more about how Locard's Exchange Principle works here: http://brando.ws/locard14 ✓

BIO

Branden R. Williams, DBA, CISSP, CISM is an ISSA Distinguished Fellow, and technology executive. He consults with global companies for digital business initiatives. Access his blog, book and contact info at www.brandenwilliams.com.