Royal Highlands Computer & Tech Club
Article – For your Reading Pleasure
Shared by Diane (Di) Binder, Club President

October 12, 2019
By James Gelinas, Komando.com

5 credit card theft hot spots that put you at risk

Credit cards have long had one big benefit, which is to save us from having to carry around wads of cash all the time. That's why using them makes shopping easier and safer — or does it?

Despite card issuers pushing new security measures every year, credit card theft is still a rampant crime. Usually these thefts are enabled by cybercrime, phishing and fraud. And today, there are more gadgets and software than ever to help the bad guys claim your info.
Regardless of where you live or how safe your computer setup, credit card theft is always possible if you're not aware of the dangers. If you tend to use plastic over paper, here's what you need to know about five threats facing you and your card accounts.

1. Sneaky skimmers

Credit card skimmers sit directly on top of ordinary credit card slots and are designed to not interfere with their normal function. You can use what seems like a normal card reader and never know your data is being swiped by a scammer.

The most common locations for credit card skimmers are gas pumps and ATMs. After hours, they're often left unmonitored, which makes it easy for criminals to install and attach a skimmer.

So how can you spot them? "Off-colored" plastic, irregular lights or awkwardly shaped readers can be a red flag, but many skimmers are so small and covert that they're tricky to spot. There are a number of different styles, such as:

Overlay skimmer: This fits over the card reader slot of an ATM or gas pump, and is designed to look like part of the covering. Watch for a slightly different color, or signs that it doesn't quite fit right.
Ultra-thin skimmers: These fit inside the card reader slot and can be much harder to detect.
Shimmer: Some are bulky and easy to spot, while others are much smaller and can fit inside the card reader. They're embedded with a microchip and flash storage that can steal the card info including your PIN.

It's easier to take steps to prevent getting skimmed rather than playing lookout. Paying a cashier at the gas station is a great way to stay clear of skimmers at a high-risk location. And use a card with an EMV chip if available, which we'll go over in the next section.

When choosing an ATM, try to stick to machines attached to your bank instead of generic units. Some banks keep ATMs locked behind doors after-hours and require your debit card to get in, which adds an extra layer of protection. These are much safer.

Keep in mind, even the most careful people can still be tricked into sharing their information. One of the best things you can do is notify the proper authorities when you notice something is wrong. Never hesitate when it comes to your safety.

2. Malicious merchants

Paying a cashier directly doesn't rule out the dangers of merchant or point-of-sale fraud. Credit card skimmers or skimming software can easily be hooked up to a register, and reports of sketchy stores doing this are not uncommon.

One of the strongest options to fight retail fraud might be in your wallet right now: the EVP chip on your credit or debit card. Not every card uses a chip, but those that do are much harder to extract data from. Most skimmers scan the magnetic strip to extract your data, so your chip card can't be copied in the same way.

You could also just opt to use cash over a card, but make sure to carry only a little more than you need. Having lots of loose bills on your person makes you more vulnerable to robberies and theft.

Don't get taken advantage of. Your private information is for your eyes only. Consider these 4 essential steps to safer online shopping and banking to protect yourself from would-be scammers.

3. Horrible hacks at popular places

Establishments like fast food restaurants are becoming higher priority targets for hackers due to the sheer volume of money that passes through their doors each day.

Carrying cash is the safest method to avoid fraud, but another strategy is to use your credit card when you're eating out or shopping instead of your debit card. Credit card limits can put a cap on how much a thief can steal at once. If a thief has access to your bank account, it's possible for them to take you all the way to zero.

Strong consumer protection laws for fraudulent credit card charges mean you'd be on the hook for $50, at most. The laws against debit card theft, though, aren't as powerful. You can challenge transactions made with your stolen card, but be prepared to wait to get your money back. And you don't alert you bank in time, you may take the entire loss on the nose.

Thieves will do whatever it takes to get your information but you don't have to be a victim. Don't sit by passively and let them steal your info. Fight back and shop smart.

4. Fear the free Wi-Fi

Everyone needs to use the internet when traveling, and hotel or coffee shop Wi-Fi is usually the default choice. When the Wi-Fi is free, that's even better, right? Well, not so much.

As we've discussed before, free Wi-Fi has a host of its own security issues. It's easy for network owners to monitor your activity, and even easier for outsiders and hackers to target the computer you use on the network. This goes double if you use free public Wi-Fi to shop or make purchases. Our advice? Wait to shop or bank until you're on a secure network.

If you can't wait, you mask your network activity with a VPN. We recommend ExpressVPN to hide your identity, protect your devices through encryption and keep hackers out.

Try ExpressVPN free for 30 days, and get 3 months free when you sign up for a year at ExpressVPN.com/Kim.

5. Evil emails infiltrating your inbox

We can't cover scams or hacks without talking about phishing — the most annoying and prolific cybercrime on the web. It's so popular because it's easy to do and requires the victim to "let the hacker in" on their own merits. It's a classic bait-and-switch for credit card and identity info.

Most commonly, phishing schemes are found in your email inbox or on a social media platform like Facebook Messenger. Sometimes, the messages look like official government forms or corporate communications. One thing they all have in common? They link to another website to trick you into entering personal information.

Regardless of what the message or website claims, never enter any personal info online unless you're certain the website is legitimate. You can usually tell by glancing at the address bar. If the url is long, complicated and doesn't contain a familiar ".com" you know and love, it might be a fake.

And remember, be wary when opening an email or message from anyone you don't know, and never follow suspicious external links or download unknown files. A sharp eye and natural skepticism is the best way to stay safe — both on and offline. Your wallet will thank you.