Places to Never Use a Debit or Credit Card to Make a Payment

By Ellen Chang

While carrying around your debit and credit cards to make your daily purchases from coffee to lunch to parking is efficient, the convenience could spell trouble.

Using your credit or debit card to pay for your purchases puts consumers at greater risk of identity theft and losing key personal information.

Here are seven places you should think twice before swiping your debit or credit card to prevent a hacker from intruding into your finances and potentially affecting your credit score.

Online Shopping

With the proliferation of discount shopping websites, make sure the online retailer you are purchasing from has a safe website, because many aren't secure. Before you enter your credit or bank card information, look for the green lock icon without any overlays, said Shaun Murphy, CEO of Private Giant, an Orlando, Florida-based company that plans to launch a security app for smartphones. "Some sites, including Amazon, will not show you a lock icon until you log-in into your account or begin the check-out process," he said. "This means anyone can see what you are shopping for while you are browsing."

Hidden/Out of View Terminals

Be wary of the hidden terminals when you are shopping. It could be the gas pump that is furthest away or an unattended station for automatic checkouts at the grocery store, Murphy said.

"These are sweet targets for credit card skimming devices that can sit there for months without anyone noticing," he said.

Nowadays, skimmers are small enough to fit inside pockets or even hidden within the credit card slots in payment terminals. This means you may unwittingly hand over data when swiping your card at a gas pump, so go inside to pay, said Geoff Sanders, CEO of LaunchKey, a Las Vegas-based decentralized mobile authentication and authorization platform.

"Criminals merely need to pull a car up in front of a pump to surreptitiously install or retrieve a skimmer within a matter of minutes," he said.

Temporary Stores

It's tempting to use your credit card to pay for a T-shirt at a concert or a vendor at a temporary open air markets, swap meets or craft fairs, "thanks to the ubiquity of mobile Internet connections," Parker said.

"These scenarios provide an excellent venue for the grifting of card information," he said. "The consumer is left trusting a vendor that doesn't have an actual retail location."

Outdoor Pay Terminals

Another place that consumers should be wary of using their cards is at outdoor pay terminals including drive through locations at fast food restaurants. Being outdoors means it's another prime location for a skimmer device to be hidden. Skimmers have even been found on the door readers that require users to scan their card before entering the ATM lobby, Parker said.

Cellphone Charging Stations

As consumers spend more time on their smartphones, charging your phone becomes more of a necessity than a preference. Even though it seems like a no-brainer to swipe your card to charge your phone for free when the battery is nearly dead, the convenience could cost you.

"These devices can also dump the information from your cellphone while charging," Murphy said. "This attack method even has a cool name: juice jacking!"

Apps

All apps aren't the same and designed with the same goal in mind. If any of the apps on your laptop, tablet or mobile device ask you for your credit card information outside of the normal app store, check to be sure the program is legit. There is a good possibility that it is a fake, especially the ones the need your immediate attention and claim that your computer has a virus or all of your files are encrypted and need to be unlocked for a price.

Free Services or Trial Period There are a multitude of free services or a trial period that allows you to watch a movie or try some software for a period of time. The catch is that you still need to enter your credit card information before you can start using it. It sounds too good to be true, because it is "almost guaranteed that the service is either going to scam you or sign you up for some paid service that will be impossible to cancel," Murphy said.

What to Use Instead of Your Bank or Credit Card

Re-loadable pre-paid cards and cash are two good options since they are not linked to any personal financial information. Using cash is the best way to avoid overspending, because it makes you more aware of the financial impact that the purchase has on your budget, said Bruce McClary, spokesperson for the National Foundation for Credit Counseling, a Washington, D.C.-based non-profit organization.

If an attacker successfully drained your checking account through your debit card, you could be without cash for quite some time.

You shouldn't use your debit card anywhere other than in an ATM machine, said Steve Weisman, a Boston lawyer and a lecturer of law, taxation and financial planning at Bentley

University in Waltham, Massachusetts. You are exposed to more liability when you are using a debit card. Although laws limit your debit card liability to $50 if you report the fraudulent use to the bank within two days,that changes as you wait longer. If you don't notice the fraud and report it to your bank after three days, your liability jumps to $500, he said.

"Your bank account will be frozen while the bank investigates the matter, thereby limiting your own access to the account," Weisman said.

If you don't have cash or a pre-paid card handy, a credit card is still a good choice because it may take banks many days to refund fraudulent charges or withdrawals, said Sanders.

"If an attacker successfully drained your checking account through your debit card, you could be without cash for quite some time," he said.

Since nearly all debit cards can be used as a credit card, consumers should always use the credit card feature, Parker said. When the card is used as a debit card with the PIN being entered, you are risk for having both the card and PIN compromised.

"This could allow cybercriminals to directly withdraw cash," he said.

With major retailers and banks such as Target, Sony, eBay, JPMorgan Chase, Home Depot, Anthem, T.J. Maxx and Apple being attacked by cybercriminals and having millions of data records leaked and exposed, consumers should be more concerned about large companies, said Dave Bennett, CTO of IONU, a data security company based in Longmont, Colorado.

"Hackers are going to go after the big targets, not the small fry," he said.

http://www.dailyfinance.com/2015/06/09/places-to-never-use-a-debit-or-credit-card-to-make-a-payment/