

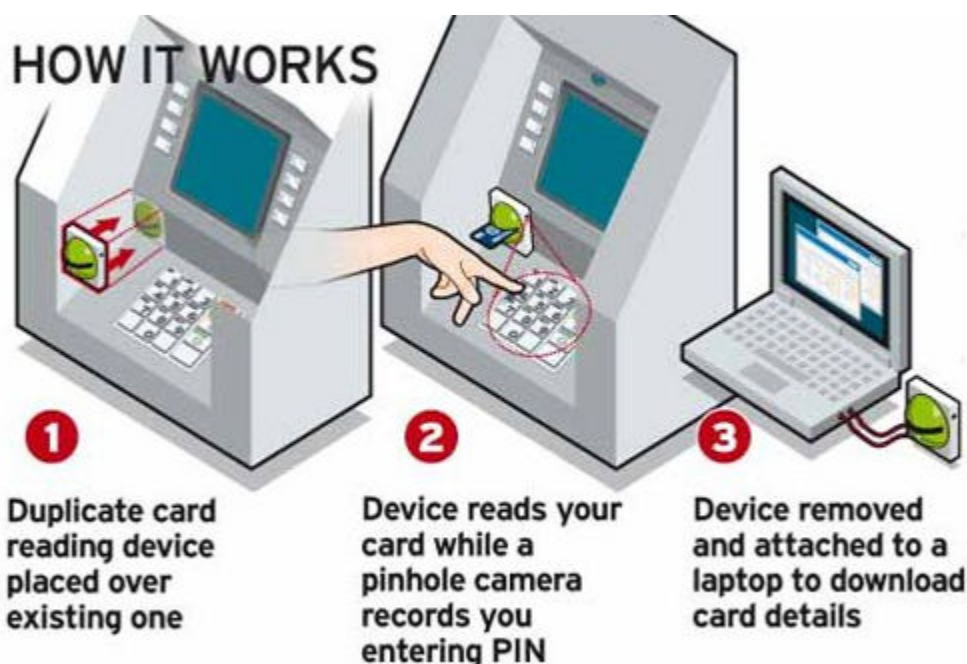
## Pegasus Protects- Card Skimming

### *February focuses on Card Skimming*

This month we shed light on the rising concern of card skimming and provide essential precautions to shield yourself from financial vulnerabilities. Stay informed, stay protected.

### **What is a Card Skimmer**

A skimmer is a device that is inserted into a card reader to collect the card number. There may also be a camera placed above or near the keypad area to record any PINs or Zip Codes entered. The fraudsters place the skimmer device over an existing card reader for a certain period of time and then retrieve it to collect the recorded information.



### *Areas where a card skimmer could be found:*

**ATM Machines:** Card skimming devices are often discreetly installed on ATMs, allowing criminals to capture card details when customers insert their cards for transactions.

**Gas Stations:** Skimmers can be affixed to card readers at gas pumps, targeting unsuspecting customers who use their cards to pay for fuel.

**Retail Point-of-Sale Terminals:** Skimming devices may be placed on card readers at checkout counters in retail stores, where customers make numerous card transactions.

**Restaurants and Bars:** Skimming devices can be concealed on handheld payment terminals or at main POS systems in hospitality establishments, putting customers' card information at risk during dining experiences.

### **How to Check for a Skimmer**

Although it may be difficult to detect, doing a visual and physical inspection can help. When using an ATM or gas pump, check for any sort of issues on the card reader and panel underneath. The panel may look not centered or at an odd angle-- take notice of any abnormalities. If it looks like it may have been tampered with, attempt to wiggle it and see if it comes out of place or moves. Card readers are manufactured with the ATM or gas pump and therefore do not move easily, so if any part seems odd or *does* move easily, use a different pump or ATM. You may also want to report it to the business housing the card reader.

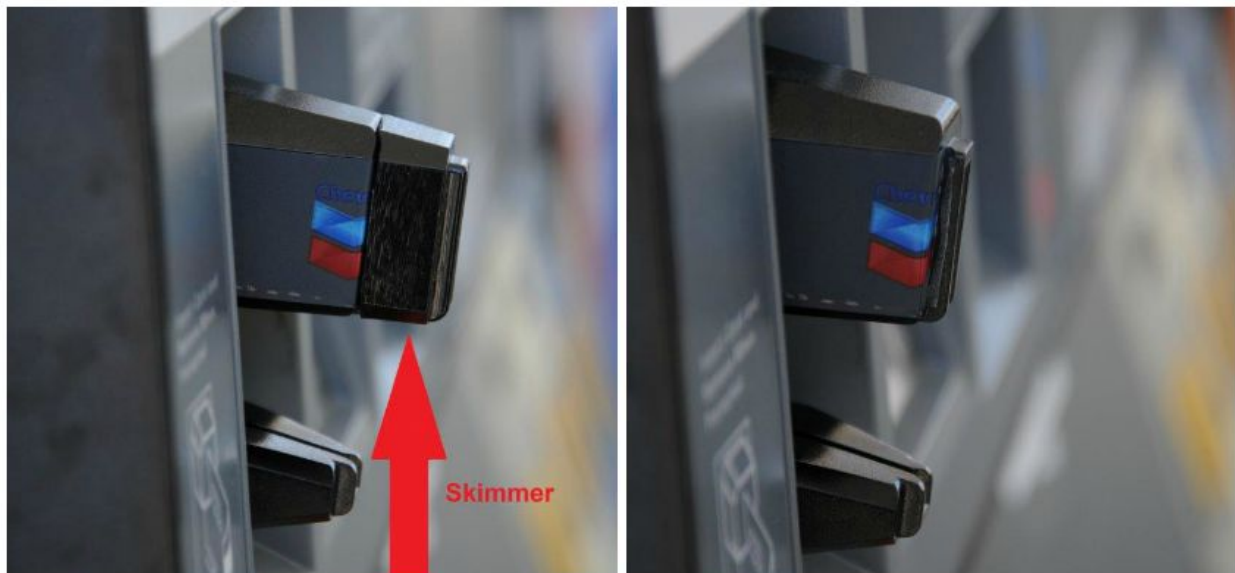


When going to retail stores, restaurants or bars try to use a contactless or chip enabled payment method so that the card does not leave your sight. This gives you an added layer of protection.

Gas pumps may have a security tape or sticker over the panel to ensure it has been screened for skimmers. If the tape looks altered, ripped, broken, or tampered with, it may be best to use a different pump.



Look inside of the card reader to see if anything is inserted and blocking your card. In some instances a light can be seen that is recording the card information. Look around the card reader for any additional light or items sticking out like in the image below.



## **How to avoid card skimmers**

*Inspect Card Readers:* Check card readers for any unusual attachments or overlays before using them.

*Use ATMs in Secure Locations:* opt for ATMs in well-lit, busy areas as they are less likely to be tampered with.

*Cover the keypad:* Shield your PIN entry with your hand to prevent hidden cameras from capturing it.

*Regularly check bank statements:* Monitor your bank statements for any unauthorized activity and report it to us immediately.

*Opt for Chip Enabled Transactions:* Use chip-enabled for transactions when possible as they provide an extra layer of security.

*Avoid suspicious ATMs:* If an ATM looks damaged or out of place, find another one.

*Keep Software Updated:* Ensure that your banking apps and security software are up to date to protect against potential vulnerabilities.

*Use contactless payments:* Consider using contactless payment methods to avoid physically inserting your card into compromised terminals.

## **What happens if a credit card is skimmed**

Thieves use the stolen card information to make their own fake cards, make purchases online or sell the stolen information on the internet.

Regularly review your credit card activity to make sure no new credit accounts have been opened, and check bank statements and online banking activity for any unauthorized transactions.

We want to remind our members to be vigilant and to review their recent transactions regularly. If you identify any suspicious activity, please contact us immediately. If you are unsure of a transaction on your debit card, turn it off momentarily with card management. Find out more through online banking or calling us.

Find more about card management here. (insert pdf)

<iframe width="560" height="315"  
src="https://www.youtube.com/embed/2n09vx3phrs?si=47J7PqzoYCchEg0" title="YouTube  
video player" frameborder="0" allow="accelerometer; autoplay; clipboard-write; encrypted-  
media; gyroscope; picture-in-picture; web-share" allowfullscreen></iframe>

Resources:

<https://www.forbes.com/advisor/credit-cards/how-to-spot-a-credit-card-skimmer/>

<https://consumer.ftc.gov/consumer-alerts/2018/08/watch-out-card-skimming-gas-pump>

<https://www.experian.com/blogs/ask-experian/what-is-card-skimming/>