SKIMMERS AND SHIMMERS

August2024 Issue 2024:8

SKIMMERS FOUND IN DELAWARE STORES

Georgetown and Felton police are investigating credit card skimming incidents at their respective cities' Dollar General stores. Two skimming devices were found within days of each other in June 2024. Both devices were discovered in the self-checkout lanes.

Felton Police said the United States Secret Service Attorney General's Office and the Montgomery County Sheriff's Office in Pennsylvania were assisting in the investigation. Police say the two agencies have expertise in conducting forensic investigations into these devices. Georgetown Police have reached out to their community partners, asking them to remain vigilant and perform regular checks of their checkout devices.

“It takes no time to place these things on there. Typically, two people, you get somebody to distract the main store associate, and then another person just snaps a device over top of the other one,” said Lt. Joel Diaz of the Georgetown Police Department, “It is typically placed over top of the original credit card machine, mimicking the machine itself. A lot of times it’s difficult to tell unless you’re really paying attention.”

Read on to learn more about how to protect yourself against skimmers and shimmers.

Solomon Adote

HOW DO SKIMMERS WORK?

A credit card skimmer is a device that can be installed illegally on ATMs, fuel pumps or point of sale (POS) systems. They can be hand-held or installed where you would expect a legitimate card reader. When customers swipe their credit or debit cards using the card reader, the skimmer can scan or skim their card information. Credit card skimmers are used to steal card data and use it for fraudulent transactions.

Tiny "skimmers" can be attached to ATMs and payment terminals to pilfer your data from the card's magnetic strip (called a "magstripe"). Even smaller "shimmers" are shimmed into card readers to attack the chips on newer cards. There's now also a digital version called e-skimming, pilfering data from payment websites.

One of the most effective ways to protect yourself is to visually inspect a card reader before using it. Look for any signs of tampering, such as loose or misaligned parts, or anything that seems out of place. Additionally, try to use ATMs or payment terminals located in well-lit, busy areas, as these are less likely to be targeted by criminals.

Another crucial step is to cover the keypad with your hand when entering your PIN. This simple action can prevent hidden cameras from capturing your PIN number. It’s also a good idea to use credit cards instead of debit cards whenever possible, as credit cards offer better fraud protection. If you must use a debit card, run it as a credit card to avoid entering your PIN. Regularly monitoring your bank statements and setting up alerts for suspicious activity can help you quickly detect unauthorized transactions.

Consider using mobile payment options or contactless payment methods, which are generally more secure than traditional card swipes. Paying inside the gas station or store, rather than at the pump or self-checkout, can also reduce the risk of encountering a skimmer. If you notice anything suspicious, report it to the store clerk or the authorities immediately. By staying vigilant and taking these precautions, you can reduce the risk of falling victim to skimmers.

Chief Security Officer

READ MORE CYBERSECURITY NEWS at DIGIKNOW!

Delaware Department of Technology & Information publishes and sends this newsletter to all network users because we need YOUR help to keep our network secure. If you are having problems viewing this message, accessing the links or want to print a PDF copy, go to:
https://digiknow.dti.delaware.gov/news/index.shtml?dc=newsletters

Department of Technology and Information
Contact us at **esecurity@delaware.gov**