@DeldigiKNOW

March 2018 Issue

DigiKnow
CYBER SECURITY DEPENDS ON YOU

eSecurity Newsletter — Credit Card Skimmers

"If something doesn't feel right about an ATM or credit card reader, just don't use it. And, whenever you can, use the chip instead of the strip on your card." - *Delaware State Police*

Gas, Cash, Skimming and Bluesnarfing: What's it all about?

WHAT ARE SKIMMERS? Skimmers are illegal card readers that steal the data from a credit card's magnetic strip. They are attached to payment terminals, gas pumps and ATMs. The skimmer grabs the data from every card that is swiped. Thieves must return to retrieve the stolen information. He or she can use the stolen data to create cloned cards or raid bank and credit card accounts.

BLUESNARFING, REALLY? Thieves have begun to use Bluetooth technology to glean credit card or debit card information. The crime is called bluesnarfing or blue skimming: Bluetooth® skimmers transmit credit and debit card information to a laptop in the crook's vehicle parked up to a 100 yards away.

WHAT'S THE RISK? 37 million Americans refuel every day — 29 million of those pay for fuel with a credit or debit card. When skimming occurs at a gas station, it usually takes place at only one pump. A single compromised pump can capture data from 30 to 100 cards per day.

Protect Yourself From Skimming

CHECK FOR TAMPERING — When you approach an ATM or any card reader, look for differences at the top, near the speakers, the side of the screen, the keyboard and in the reader itself. If something looks different, like color, material, graphics that are misaligned, DON'T USE THE MACHINE!

WIGGLE EVERYTHING — Push/pull at everything. ATMs should NOT jiggle or have any loose parts. Check that the keyboard is securely attached and just one piece. Be wary if it seems difficult to insert your card.

USE COMMON SENSE — Avoid gas pumps that are out of sight of the clerk and ATMs in areas with little traffic. It's particularly important to be cautious at independently-located ATMs, such as those found in convenience stores, entertainment venues or nightclubs. Non-bank ATMs accounted for the majority of compromised devices in 2016.

STAY AWARE — Whenever you enter your PIN or ZIP Code, assume someone is watching. Simply concealing your hand while you enter the number can safeguard your keystrokes. Timely reporting is important in fraud cases. Keep an eye on all of your financial statements; identify and report transactions you don't recognize.

HERE'S A BASIC TAKEAWAY: use your credit cards and lessen your reliance on debit cards. If a thief makes a charge on your credit card that you didn't authorize, a simple phone call can fix the problem. If the crooks manage to siphon all cash from your checking account, that's a bigger problem that could take several days to sort out with the bank (and longer if you count any other businesses you may have just paid with a check).

Visit the DTI eSecurity website for previous issues
eSecurity Newsletters

Questions, comments or topic suggestions?
Email us at eSecurity@state.de.us.

DEPARTMENT OF TECHNOLOGY & INFORMATION
DELIVERING TECHNOLOGY THAT INNOVATES

Delaware Department of Technology and 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.