VISTA ROYALE COMPUTER CLUB

Meeting Minutes 1/18/2024

Linda Briggs, President, welcomed 38 new and returning members to the third meeting of the 2024 season. She also announced the Public Budget Meeting noted below. Sandy McKenny will let Nancy, Sec., know of any genealogy announcements she has for club members and they will become part of the meeting minutes.

VR Association Announcements:

01.24.2024 Public Budget Meeting at RPCC 9:00 a.m. - 11:00 a.m.

All owners are welcome to attend

Upcoming VRCC Meetings:

Jan 25 Amy Shoemaker - McKee Gardens - Amy's presentation will include an explanation of the McKee Children's Garden.

Feb 01 Indian River Sheriff Dept.

Feb 08 ACT/Jurgen Schwanitz - Building Gaming Machines

Feb 15 IPHONES for senior dummies - Linda Briggs

Feb 22 TBA

Feb 29 TBA

Mar 07 Estate Planning - Pamela Hennig

Mar 14 ACT/Jurgen Schwanitz - Cyber Security

Mar 21 TBA

Mar 28 Linda Briggs

Programs always begin at 9:30 a.m. and are held in the Pine Arbor Clubhouse kitchen

Twelve consecutive weekly programs are scheduled - every Thursday between 1/4/24 - 3/28/24

Shout Out to ALL MEMBERS - Thank you for supporting VRCC, now in its 22nd year of serving the Vista Royale community!

Membership Fee Sign Up Details:

2 For 1 through January 31 @the LAB

$20 (cash only) + proximity badge to sign up ($20 for 2 people) .

Genealogy Opportunity in Vero Beach:

Presenter: Lisa Louise Cook

March 23, 2024

Our History- Your Story

Indian River County Library

1600 21st Street

Vero Beach

TODAY'S PROGRAM, JANUARY 18, 2024

Vicky Getz, Meeting Presenter

General Payment Card Safety

Tap & Pay Scams Skimming Shimming

Vicky started off with a hot scam topic -- bank impersonation. Most people lose around $3000, or more, when they fall for it. The amount of pain you are going to feel when your card is compromised depends greatly on what kind of card is hacked and how soon you discover the activity. Always keep an eye on card activity and report problems immediately. As Vicky informed, the pain of fraud when your credit card number is used for unauthorized transactions is annoying but it doesn't sting compared to the likes of bank impersonation. Bank account fraud (impersonation) is very time consuming and difficult to resolve. Bank fraudsters are aiming to gain access to your checking account. It is important to take all safety precautions when using an ATM machine. (See Vicky's notes below for specific tips for less risk and more safety when using both debit and credit cards.)

If you must use your debit card for point of sale, choose to use it as a CREDIT card. A Skimmer fits over the normal card reader. It's in front and a lot of things are done internally. Gas pumps are a good example of this - see link to video below. Point of sale skimmers are a little bit wider and taller to fit over other machines - see link to video below.

Have you heard about local skimming or shimming outbreaks? Beware! That's when it's time to really pay attention and be intentionally cautious when paying out or withdrawing cash at an ATM. Please note that there is a wide variety of skimmers and shimmers out there. The idea is to be observant and diligent about keeping fraudsters at bay.

Vero Beach's Walmart Neighborhood Store does not have the tap to pay option. Swipe and insert are the two options and the machines are protected with a very obvious BLUE sticker on the side of each machine. The machines are safety checked each morning and a new blue sticker is put in place before the store opens for business.

Vicky's #1 piece of advice - PROTECT THE PIN! Look at card readers and check for them being loose or damaged. If they are, don't use them.

Hood the ATM machine with your hands when entering your PIN number. RFID uses less information and avoids skimmers and shimmers.

When a customer slides a card to pay or withdraw money, the skimmer copies the card's information from the magnetic strip on the back of the card. Newer devices, called shimmers, also can copy the data from the card's chip after it's slotted into the machine.

Tap to Pay not working.....? 🤔 **Sometimes it will stop working if the card has been tapped too many times in a row. A couple of fixes for this - simply hold the card in tap position. If that doesn't do it, you may need to insert the card to pay. The tap and pay should work the next time the card is used.**

We learned that mobile phone payments should be safer than credit card payments - Google Pay, Apple Pay, Samsung Pay, etc. and that Face ID is great and very safe technology if you are a safe user.

As always, the best situation is to come to VRCC's weekly meetings to catch all the details and extras. Equally important, the meetings afford all of us a social outlet and an easy way to connect with other VR residents. There's nothing like being engaged in the process!

Come join us Thursday, January 25th to hear all about McKee Gardens (Children's Garden, too)

Amy Shoemaker - guest speaker

9:30 a.m. PACH -- bring along a Vista friend. Thank you for your participation and support of the VRCC. 👏

See you there!

Nancy Dalley

Secretary

Please find Vicky's informative and very useful notes below from today's meeting, including several links to short videos we watched together at the meeting.

General Payment Card Safety

Skimming & Shimming

Credit vs Debit Cards

Tap to Pay

RFID Protection

Wireless ATM LogOut

Fraud vs Authorized Transactions

Bank Impersonation Scams

Have you been a victim?

About 400,000 Americans experience some kind of card fraud each year.

The amount of pain you feel when your card is compromised depends greatly on what kind of card was hacked and how soon you discover the fraudulent activity.

KEEP AN EYE ON THE ACTIVITY IN YOUR ACCOUNTS and report problems immediately.

Fraud is when a stolen card number is used for an unauthorized transactions

When you discover an unauthorized transaction occurred on your credit card, usually you have lost no money. You report the fraud, get a credit on your statement, get a new card and the issue will never affect your bank account. Maximum liability $50.

With a bank debit card, your bank balance is reduced immediately. If the transactions are significant, you could experience a domino of late charges and overdraft fees while you fight with your bank to get the money refunded to your account.

We watched this video on skimming https://www.youtube.com/watch?v=WfqZAActw90

Skimming increased 750% in 2022

Skimming doubled again in 2023

In 2014 we changed to EMV chip cards to prevent skimming. By 2016 criminals had moved on to using shims, small devices inside the credit card slot, to capture the EMV chip data.

The problem at gas pumps was so problematic, that Florida has enacted new laws that require gas stations to inspect their pumps more often.

https://www.youtube.com/watch?v=qM3dN9UoSEo

In 2018 new Point of Sale (POS) skimmers started appearing in Mexico.

https://www.youtube.com/watch?v=q3PfUjWmLFg

The new Point of Sale (POS) Skimmer is hard to spot, and has a paper thin card reader powered by the insertion of a chip enabled credit card. They capture the pin and everything needed to create a magnetic strip on a credit card. The thieves retrieve the information by inserting a smart card that can dump all the information on your card. If your card was a debit card, the smart card now has what the thieves need to get into your bank account.

Contactless Payments have an advantage in that they never come in contact with the skimmers and shimmers and pass less information. If offered, opt for tap to pay instead of inserting your card.

Contactless payments include Tap to Pay credit cards, or using Mobile Phone Apps, like Apple Pay, Google Pay or Samsung Pay

Radio Frequency Identification (RFID)

RFID is used for tap to pay. It sends less information and avoids contact with skimmers and shimmers.

https://www.youtube.com/watch?v=9Q9Mz_QJJsM

An RFID Pickpocket with special equipment or a special app on their phone can read the data emitting from your cards. Typically they can pick up the credit Card Number and expiration date. Sometimes some cards may give your name or the last 10 transactions you made as well. There is a whole industry offering RFID protecting clothing, wallets, purses and credit card sleeves guarding against RFID Pickpockets.

While RFID pickpocketing is rare, aggressive Tap To Pay terminals are not.

https://abc7news.com/technology/customers-say-tap-to-pay-charged-their-card-through-bags-pockets/13155986/

RFID sleeves are easy to come by. Vicky recommends buying a pack of RFID credit card protection sleeves with a variety of colors to identify the card you are looking for. Vicky showed her Deezomo sleeves which she bought because they were pretty and the reviews were good.

Mobile Phone Payments

Should be safer than credit cards. There have been no major breaches reported, so far.

The biggest security risk to mobile pay platforms is the individual using the mobile device.

Password fidelity, never use public wifi, never let anybody handle your unlocked phone, never let anybody see when you tap your pin, be totally aware of the current scams and how to avoid them ...

When a stolen card number is used for an

Using a Credit instead of Debit insulates your bank account from fraud. If you are carrying credit card debt, credit cards can

ATMs are targets too. ATM's at convenience centers are 70% more likely to be compromised than ATM's at banks.

https://www.youtube.com/watch?v=I1GKlWU_wZ4

In 2016 Vero Beach ATMs were skimmed/

https://youtu.be/OmzgL_XE9jI?si=t4K8JBB9jGm9Dnyu

Many banks in the area such as Chase, Seacoast and Wells Fargo offer touchless ATMS. Others do not.

Touchless ATMs are safer ONLY IF You know how to use them! The next video shows how failure to log out of an ATM can cost you serious coin! We couldn't pull this one up in the meeting.

https://abc7.com/chase-bank-atm-scam-tap-to-pay/12913307/

Electronic Fund Transfer Act

Debit Card Protection

In the United States, Regulation E (Reg E), which was issued by the Federal Reserve as an implementation of the Electronic Fund Transfer Act of 1978, determines the conditions under which financial institutions will reimburse their customers for unauthorized electronic transfers. While several clarifications have been issued over the years to outline specific cases for online banking and debit card activity, one thing remains clear — If a customer performed an authorized transaction even if they were manipulated to do so by a scammer, they will not be covered under Reg E and the bank will not be liable to reimburse customers.

https://youtu.be/a?si=0XrXy7vot9Gdv0VO

`

BANK ALERTS

Alerts from major banks do not come from a ten digit phone number nor an email!! They come from the bank's 5 or 6 digit short code.

FEAR or IMMEDIATE ACTION

Beware of any text, email or phone call that requires immediate action involving your account, it more than likely is a scam. Don't click on links, or use any of the contact information provided in the fraud alerts. Always initiate contact with the bank from a verified source like the number on the back of your card, or from your contacts, or from your stored bookmarks. Do not believe caller ID. Banks will never ask for your PIN or your 2 factor verification code when they try to verify your identity over the phone. Banks will never have you transfer your money to another account to keep it safe.

General Card Safety

If you can, use a Credit Card instead of a Debit Card.

Credit cards offer better fraud protection.

Sign up for fraud alerts on your cards.

Actively track your bank and credit card activity!

Learn how to handle a fraud alert safely!

If offered, use a Contactless payment method, instead of inserting your card.

Log out of Contactless ATM Transactions

<u>Authorized transactions are not protected by the Electronics Fund Transfer Act.</u>

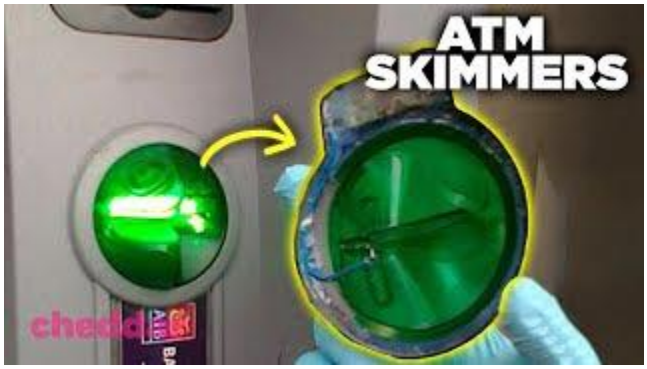
Use RFID protection on your cards and your passport and enhanced drivers license.

Fake bank fraud alerts are the #1 SMS (texting) scam in the county. The average victim loses $3000.

KEEP AN EYE ON THE ACTIVITY IN YOUR ACCOUNTS and report problems immediately.

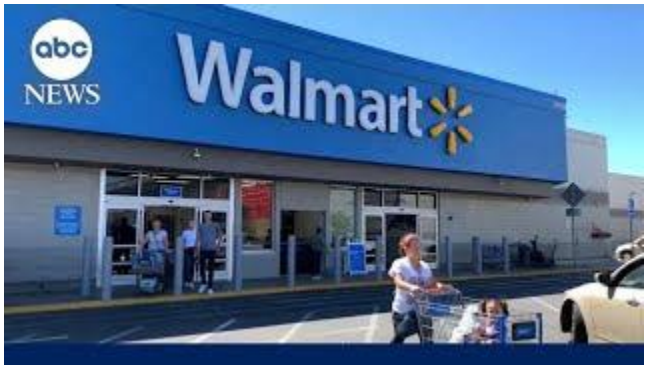
Attachments area

Preview YouTube video ATM Skimmers: Fear Mongering Or A Real Threat? - Cheddar Explains



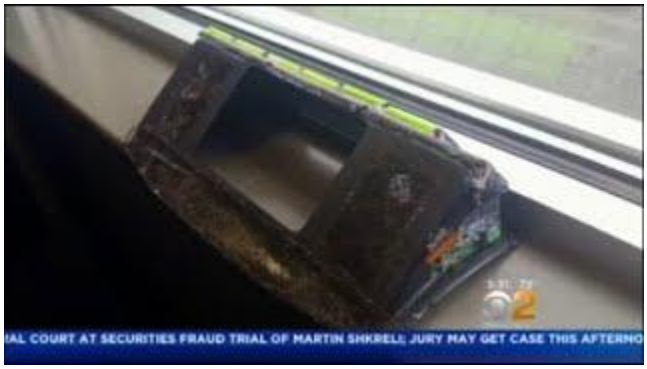
Preview YouTube video Florida law holds gas stations accountable for skimmers found in pumps

Preview YouTube video Credit card skimmers found in Walmart checkouts l GMA



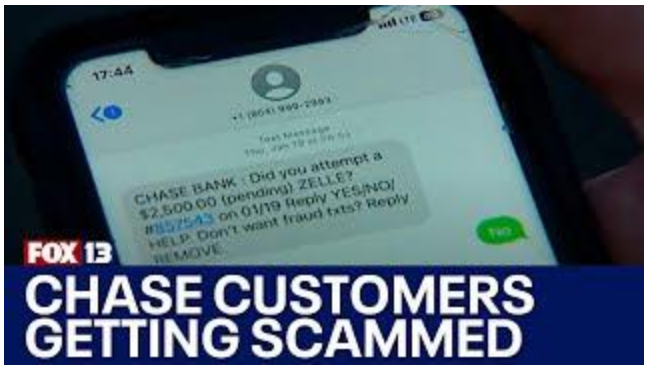
Preview YouTube video How to tap to pay with Visa (contactless cards)

Preview YouTube video ATM Skimmer Found In Queens



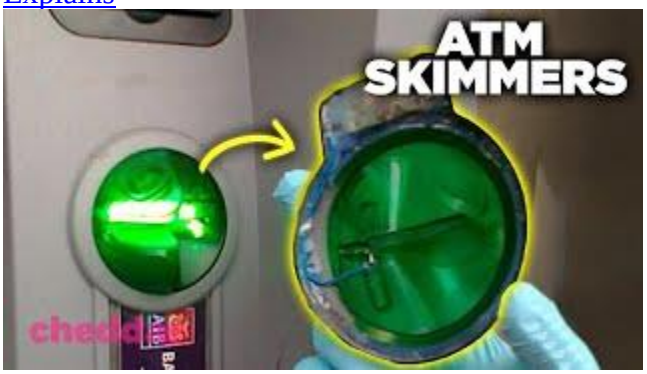
Preview YouTube video Five skimmer devices found on bank ATMs in Indian River County

Preview YouTube video Chase customers outraged after reports of scams continue | FOX 13 Seattle



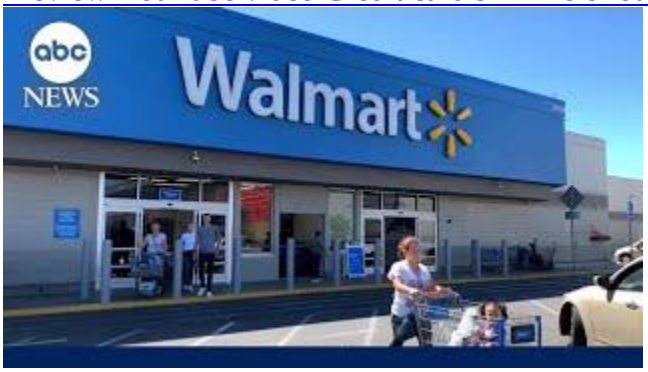
Attachments area

Preview YouTube video ATM Skimmers: Fear Mongering Or A Real Threat? - Cheddar Explains



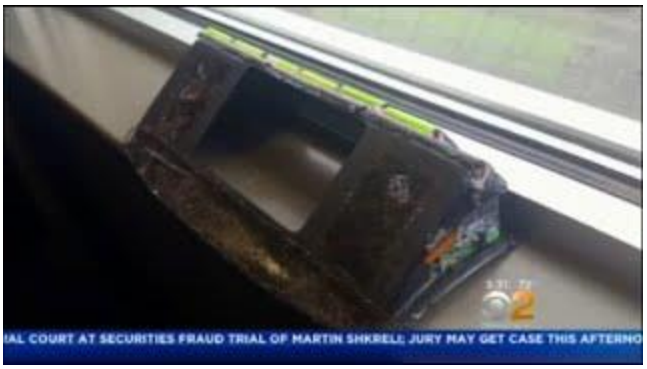
Preview YouTube video Florida law holds gas stations accountable for skimmers found in pumps

Preview YouTube video Credit card skimmers found in Walmart checkouts l GMA



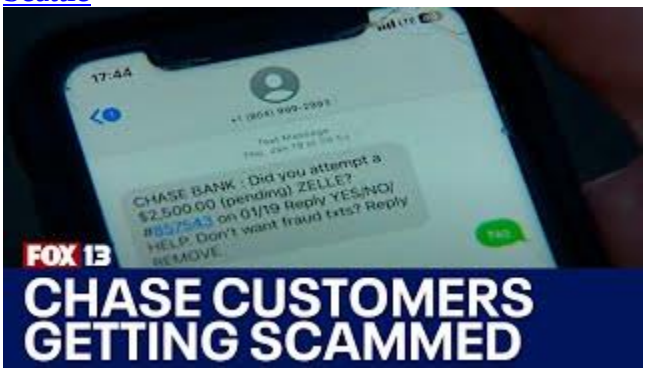
Preview YouTube video How to tap to pay with Visa (contactless cards)

Preview YouTube video ATM Skimmer Found In Queens



Preview YouTube video Five skimmer devices found on bank ATMs in Indian River County

Preview YouTube video Chase customers outraged after reports of scams continue | FOX 13 Seattle



S