ICJE News for You

1 message

ICJE, Inc. <jimrechel@icje.org>
Reply-To: jimrechel@icje.org
To: pcalvert@faulkner.edu

Wed, Dec 1, 2021 at 10:09 PM

December 2021

INSTITUTE FOR CRIMINAL JUSTICE EDUCATION

Your Monthly News & Updates

Visit the ICJE Website

"Where Are You Christmas?"

With all of the angst in the world, I thought the lyrics of a song Faith Hill recorded years ago would be the best medicine I could recommend to deal with all the discord being fermented in our lives.

Where are you Christmas
Why can't I find you
Why have you gone away
Where is the laughter
You used to bring me
Why can't I hear music play

My world is changing
I'm rearranging
Does that mean Christmas changes too

Where are you Christmas
Do you remember
The one you used to know

I'm not the same one
See what the time's done
Is that why you have let me go

Christmas is here
Everywhere, oh
Christmas is here
If you care, oh

If there is love in your heart and your mind
You will feel like Christmas all the time *

May the Spirit of Christmas be the greatest gift you give, and receive, this holiday season.

From everyone at ICJE, Merry Christmas and Happy Holidays!

Jim Rechel
ICJE Newsletter Editor

*"Where Are You Christmas" is a song co-written by James Horner and Will Jennings for the movie How the Grinch Stole Christmas in 2000.

Staying Safe...Triple-A Plan (*Not Associated with AAA*)

Staying Safe in an Unsafe World - Part 2

The Triple-A Plan: Avoidance and Counter-Surveillance

As I was beginning to write this series, I went to my local barbershop for a haircut. I was talking with another customer, a retired deputy, when a person who looked unkempt and homeless entered the barbershop, slammed the door, and began muttering to himself. I instinctively looked for a weapon bulge on the individual but didn't see one, so I wasn't too concerned, thinking that this was just another soul who "had issues."

When our barber took the next customer, the individual became irate, claiming that he was next and cursing all those present. He then stormed out of the shop. I watched him leave and walk across the parking lot. The retired deputy moved so that he could see the person if he returned.

After the incident, and as we were talking to the barber, he said he wasn't worried because he knew we would protect him. Both of us laughed at that, saying that, on the contrary, our concern was whether we could get out the back entrance fast enough if the guy returned.

Lessons Learned:

As we understand the necessity for practicing situational awareness in our daily lives, we also need to avoid the trap of Cognitive Dissonance; that is, believing something but acting in opposition to our beliefs. Examples are not taking threats seriously, understanding there is a threat but thinking that it wouldn't happen to us (not in our backyard), or thinking that because an incident hasn't yet happened, it simply won't happen.

A typical example is found in this short video of a shooting event. The video may be viewed in our Screencast streaming account, link below. Watch the man in the light blue sportscoat and tan pants closely: https://www.screencast.com/t/Uj3VRFhIOB

When you hear gunshots and your instincts tell you that there is imminent danger, you should know to remove yourself from the threat; however, this person obviously follows his curiosity rather than his better instincts.

Avoidance Tactics:

1. When in public places, walk with your head up, and never walk while looking at a cell phone.

2. Always stay alert in public. Most public attacks can be avoided if the victims are simply aware of their surroundings.

3. Always remain in well-traveled public areas. At night, stick to well-lighted areas. Just like the lions shown in the nature videos, most predators pick those on the outside of the herd. You want to remain in the middle of the pack where there is greater safety.

4. When walking in public, pause and occasionally turn, noting the persons around you. Often, predators will stop or lose interest when they realize they are observed.

5. If someone is following you, consider confronting them. This tactic is contrary to our normal instincts, and not everyone can or should do this, but it can be very effective in startling a would-be attacker and thereby preventing an attack.

6. Change your behavior: Don’t walk or run the same route, and don’t drive the same road, especially to and from work or school.

7. When driving, check the vehicles following you. If they follow you through more turns than normal, consider driving toward the nearest police precinct.

8. In a restaurant or business, always sit where you can observe the entrance and those who are entering. Also, observe and choose alternate exits if you are faced with a dangerous situation.

Summary: We often are aware of danger signals but suppress the signals through curiosity, inertia, or disbelief. Act on your instincts. Also, review the eight avoidance tactics outlined above and make a habit of incorporating them into your daily life experience.

Next month we will offer tips for making your home a harder target, offering greater protection from home invasions, burglaries, and thefts.

For comments or suggestions, please get in touch with us at training@icje.org.

Thanks, and stay vigilant.
Bob Thetford
ICJE, Inc.

"Follow Home" Robberies Surging

Last year a former neighbor was grocery shopping at a nearby Kroger's store. She loaded her groceries in her car, in the middle of the afternoon. Unbeknown to her, predators were lurking in the parking lot, looking for potential victims. They followed her home and confronted her as she was carrying her groceries into her house. They pulled a gun and robbed her of her purse and forced her inside where they stole more personal items.

At the time, we never knew this type of crime would grow to the level it has in many large cities in states across America. In Los Angeles the surge is so great they have had to form a task force to address the issue.

If it hasn't happened in your community yet, unfortunately it will.

From LAWeekly.com

MORE THAN 100 ‘FOLLOW-HOME ROBBERIES’ BEING INVESTIGATED IN LOS ANGELES

ISAI ROCHANOVEMBER 17, 2021

Days after LAPD alerted communities of a rise in street robberies, the dept. revealed it is investigating at least 110 “follow-home robberies.”

The follow-home robberies involve Angelenos being followed home after patronizing chic areas such as shops on Melrose Avenue, the Jewelry District in downtown L.A. and high-end restaurants/night clubs in the city. The suspected robbers are said to target people based on their jewelry and type of car driven.

“In early 2021, Los Angeles Police Department Robbery-Homicide division, Robbery Special Section identified an ongoing crime trend of follow-home robberies,” LAPD said in a Nov. 12 news release. “It is our opinion that these crimes are all a trend, similar to the trend experienced a year ago with the ‘knock knock’ burglaries in which different crews/gangs participated in the same type of residential burglary.”

LAPD said in past incidents where suspects have been arrested, they have found a link between at least six different gangs.

People who frequent these upscale areas are being asked by LAPD to take measures such as being aware of their surroundings, not display valuable jewelry and call 911 if they believe they are being followed. LAPD also asked people to comply with the robbers and write down all information they can remember as far as descriptions of the suspects and possible vehicles.

Los Angeles Police Department
Los Angeles, California

News Release

November 12, 2021 **NR21317ml**

Follow-Home Robberies

Los Angeles: Detectives from the Los Angeles Police Department's Robbery Homicide Division (RHD), Robbery Special Section, are seeking the public's help in providing any information that would lead to the identification and arrest of suspects responsible for follow home robberies.

In early 2021, Los Angeles Police Department Robbery-Homicide Division, Robbery Special Section, identified an ongoing crime trend of follow-home robberies. Suspects would target victims in Los Angeles, following them, and then commit the robberies as the victims were arriving home or to their business. As a result of this, RHD detectives began to track the various robberies that were being reported.

In this trend, detectives noted that victims were being followed from such places like Melrose Avenue, the Jewelry District of Los Angeles, high-end restaurants, and nightclubs from Hollywood and Wilshire Area. Victims were being targeted based on the jewelry they were wearing and/or the car they were driving.

To date, RHD detectives have identified over 110 incidents. In reviewing these reports and speaking with area detectives, it is clear that not all these incidents are related, in terms of the same suspects committing these crimes.

This conclusion is based in part on the suspects background (in those cases were arrests have been made or suspects identified) and their gang affiliations. It should be noted that out of the 110 incidents being tracked, 107 involve suspects identified as male Blacks. In three of the cases the suspects are identified as male Hispanics.

RHD identified and assumed the investigative responsibility of several series. In these series, at least six different LA street gangs have been identified.

It is our opinion that these crimes are all a trend, similar to the trend experienced a year or two ago with the "knock-knock" burglaries in which different crews/gangs participated in the same type of residential burglary.

The investigation is ongoing and anyone with information regarding these incident is urged to contact RHD at (213) 486-6840. During non-business hours or on weekends, calls should be directed to 1-877-LAPD-24-7 (1-877-527-3247). Anyone wishing to remain anonymous should call Crime Stoppers at 1-800-222-TIPS (800-222-8477). Tipsters may also go to www.lapdonline.org and click on "Anonymous Web Tips."

###

The ‘Zelle Fraud’ Scam: How it Works, How to Fight Back

November 19, 2021

One of the more common ways cybercriminals cash out access to bank accounts involves draining the victim’s funds via Zelle, a “peer-to-peer” (P2P) payment service used by many financial institutions that allows customers to quickly send cash to friends and family. Naturally, a great deal of phishing schemes that precede these bank account takeovers begin with a spoofed text message from the target’s bank warning about a suspicious Zelle transfer. What follows is a deep dive into how this increasingly clever Zelle fraud scam typically works, and what victims can do about it.

Scammers are blasting out text messages about suspicious bank transfers as a pretext for immediately calling and scamming anyone who responds via text.

Anyone who responds “yes,” “no” or at all will very soon after receive a phone call from a scammer pretending to be from the financial institution’s fraud department. The caller’s number will be spoofed so that it appears to be coming from the victim’s bank.

To “verify the identity” of the customer, the fraudster asks for their online banking username, and then tells the customer to read back a passcode sent via text or email. In reality, the fraudster initiates a transaction — such as the “forgot password” feature on the financial institution’s site — which is what generates the authentication passcode delivered to the member.

Ken Otsuka is a senior risk consultant at CUNA Mutual Group, an insurance company that provides financial services to credit unions. Otsuka said a phone fraudster typically will say something like, “Before I get into the details, I need to verify that I’m speaking to the right person.

What’s your username?”

“In the background, they’re using the username with the forgot password feature, and that’s going to generate one of these two-factor authentication passcodes,” Otsuka said. “Then the fraudster will say, ‘I’m going to send you the password and you’re going to read it back to me over the phone.'”

The fraudster then uses the code to complete the password reset process, and then changes the victim’s online banking password. The fraudster then uses Zelle to transfer the victim’s funds to others.

An important aspect of this scam is that the fraudsters never even need to know or phish the victim’s password. By sharing their username and reading back the one-time code sent to them via email, the victim is allowing the fraudster to reset their online banking password.

Otsuka said in far too many account takeover cases, the victim has never even heard of Zelle, nor did they realize they could move money that way.

“The thing is, many credit unions offer it by default as part of online banking,” Otsuka said. “Members don’t have to request to use Zelle. It’s just there, and with a lot of members targeted in these scams, although they’d legitimately enrolled in online banking, they’d never used Zelle before.”

Otsuka said credit unions offering other peer-to-peer banking products have also been targeted, but that fraudsters prefer to target Zelle due to the speed of the payments.

“The fraud losses can escalate quickly due to the sheer number of members that can be targeted on a single day over the course of consecutive days,” Otsuka said.

To combat this scam Zelle introduced out-of-band authentication with transaction details. This involves sending the member a text containing the details of a Zelle transfer – payee and dollar amount – that is initiated by the member. The member must authorize the transfer by replying to the text.

Unfortunately, Otsuka said, the scammers are defeating this layered security control as well.

“The fraudsters follow the same tactics except they may keep the members on the phone after getting their username and 2-step authentication passcode to login to the accounts,” he said. “The fraudster tells the member they will receive a text containing details of a Zelle transfer and the member must authorize the transaction under the guise that it is for reversing the fraudulent debit card transaction(s).”

In this scenario, the fraudster actually enters a Zelle transfer that triggers the following text to the member, which the member is asked to authorize:

For example:
“Send $200 Zelle payment to Boris Badenov? Reply YES to send, NO to cancel. ABC Credit Union . STOP to end all messages.”

“My team has consulted with several credit unions that rolled Zelle out or are planning to introduce Zelle,” Otsuka said. “We found that several credit unions were hit with the scam the same month they rolled it out.”

The upshot of all this is that many financial institutions will claim they’re not required to reimburse the customer for financial losses related to these voice phishing schemes. Bob Sullivan, a veteran journalist who writes about fraud and consumer issues, says in many cases banks are giving customers incorrect and self-serving opinions after the thefts.

“Consumers — many who never ever realized they had a Zelle account – then call their banks, expecting they’ll be covered by credit-card-like protections, only to face disappointment and in some cases, financial ruin,” Sullivan wrote in a recent Substack post. “Consumers who suffer unauthorized transactions are entitled to Regulation E protection, and banks are required to refund the stolen money. This isn’t a controversial opinion, and it was recently affirmed by the CFPB here. If you are reading this story and fighting with your bank, start by providing that link to the financial institution.”

“If a criminal initiates a Zelle transfer — even if the criminal manipulates a victim into sharing login credentials — that fraud is covered by Regulation E, and banks should restore the stolen funds,” Sullivan said. “If a consumer initiates the transfer under false pretenses, the case for redress is more weak.”

Sullivan notes that the Consumer Financial Protection Bureau (CFPB) recently announced it was conducting a probe into companies operating payments systems in the United States, with a special focus on platforms that offer fast, person-to-person payments.

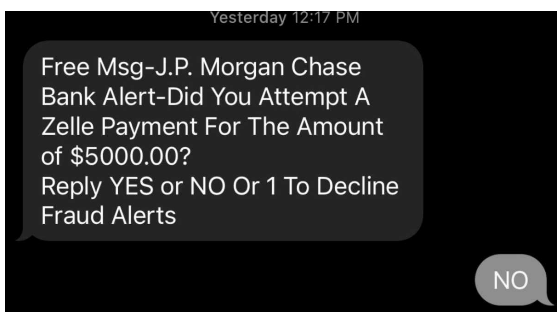
“Consumers expect certain assurances when dealing with companies that move their money,” the CFPB said in its Oct. 21 notice. “They expect to be protected from fraud and payments made in error, for their data and privacy to be protected and not shared without their consent, to have responsive customer service, and to be treated equally under relevant law. The orders seek to understand the robustness with which payment platforms prioritize consumer protection under law.”

Anyone interested in letting the CFPB know about a fraud scam that abused a P2P payment platform like Zelle, Cashapp, or Venmo, for example, should send an email describing the incident to BigTechPaymentsInquiry@cfpb.gov. Be sure to include Docket No. CFPB-2021-0017 in the subject line of the message.

In the meantime, remember the mantra: Hang up, Look Up, and Call Back. If you receive a call from someone warning about fraud, hang up. If you believe the call might be legitimate, look up the number of the organization supposedly calling you, and call them back.

This entry was posted on Krebsonsecurity.com Friday 19th of November 2021 04:36 PM

An example of an actual fraudulent text:



ICJE Training Opportunities

ICJE Training Schedule

While the 2021 calendar was full of dates, we still cannot publish our end of year training schedule as we are still awaiting word from ADECA and AUM regarding the necessary grant approvals in order for ICJE to post training classes moving forward. We have plenty in the stable, and will post them as soon as we get the go ahead!

We'll keep you posted!

STILL WAITING FOR GRANT APPROVAL :(

For more information and registration links go to: ICJE - Institute for Criminal Justice Education, Inc.

Thought of the Month

"The American Republic will endure until the day Congress discovers that it can bribe the public with the public's money."

— Alexis de Tocqueville

Alexis-Charles-Henri Clérel de Tocqueville (July 29, 1805 – April 16, 1859) was a French political thinker and historian best known for his Democracy in America (appearing in two volumes: 1835 and 1840) and The Old Regime and the Revolution (1856). In both of these works, he explored the effects of the rising equality of social conditions on the individual and the state in western societies.