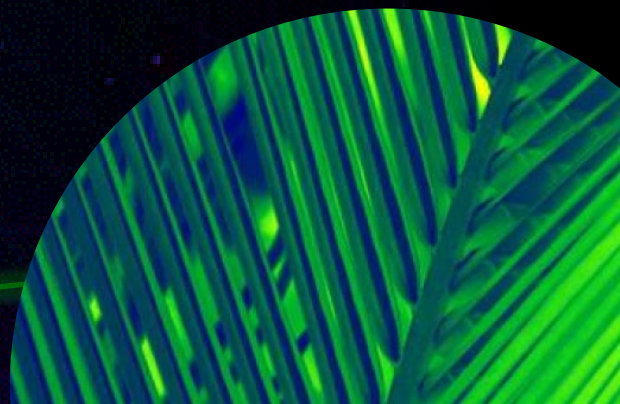
OSINT ADVENTURES

WHO CASHED MY CHECK?!

Catching (Very Obvious) Fraudsters



Presented by Squiddy for DCGVR @ DEF CON 32

ABOUT ME

- OSINT Enthusiast
- Lesbian Feminist and Professional Internet Yapper
- Medical Laboratory Scientist, MLS, MHIS
- Desktop Engineer, Hacker, Small Business Owner,

Blah blah blah..

SQUIDEYE

Small business in Champaign-Urbana, formed in February 2024. SquidEye is an electronics repair shop that aims to be affordable and accessible to the community. SquidEye functions as a queer-friendly space and mini-Makerspace. Often, because of my OSINT background and willingness to try fixing just about anything, people bring me all sorts of tasks, problems, and questions.

I've been asked to fix phones, toasters, plush toys, design websites, clean playstations, find deleted webpages, bait hackers, locate pedophiles with active arrest warrants, and catch scammers.

I've also been commissioned to light up some funky mushroom art.

I've been shocked more times than I can count, grabbed a live wire and had my hair (eyelashes included) burnt off, accidentally set fire to things, been covered in broken glass, and nebulized after inhaling a fair bit of spray paint during an art escapade at 2AM.

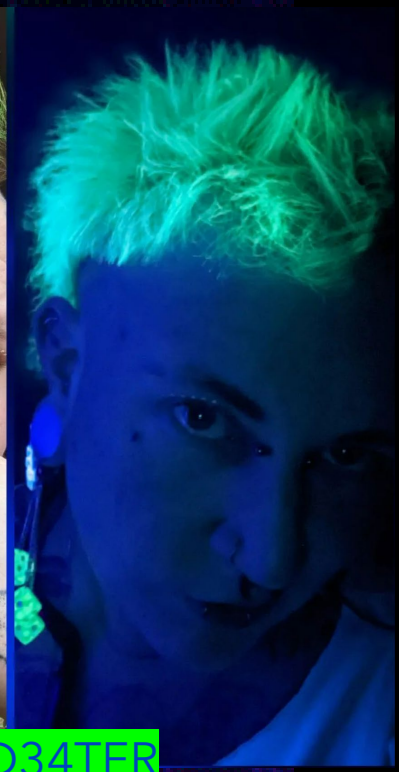
I wouldn't change a thing, but my wife wants to ground me. ☹

BIRD34TER

I rent shop space at Bird34ter - a local, queer art studio and hair salon run by Xed (“Eddie”) Boatz, AKA Bird34ter. The “pit” where hair-cutting transformation takes place is fidget-filled, and sensory-friendly.

Apart from being a very talented mixed-media artist, Xed does all sorts of amazing things with hair. If you’re ever in Champaign-Urbana, come get the gayest haircut of your life while you check out their art.

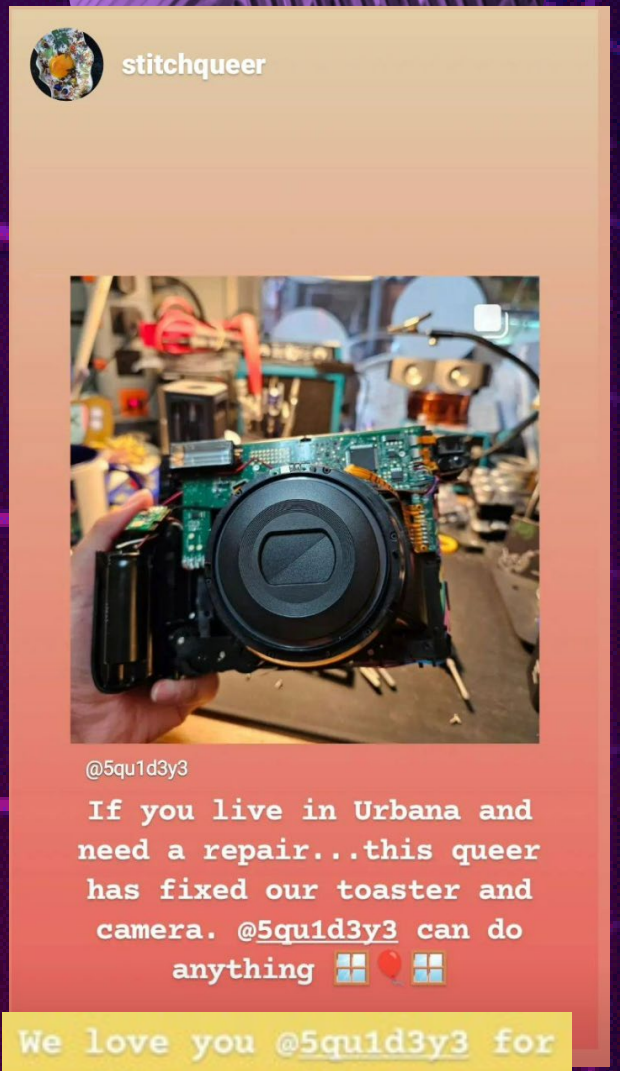
Give them a follow on social media to support a small-business!

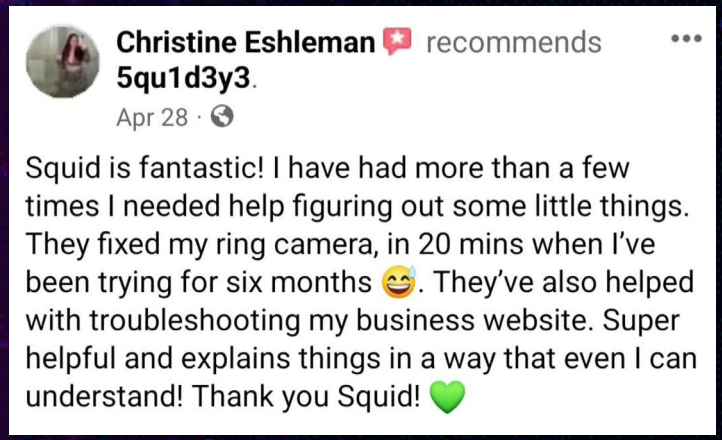


BIRD34TER

HELPING OUT

I worked a handful of jobs before SquidEye's official open date in June and have received some very positive reviews.





In April, I received an interesting request from another local, small business connection who had been targeted by small-time criminals:

Help me catch these frauds!

AN INTERESTING JOB

HOW'D THE $TORY GO?

A business owner received communication from their electric company that they were facing possible disconnection due to their last payment not being received, despite the owner attempting to pay their electric company via their bank's mobile app. When the owner called the bank, the bank informed the owner that they had received "electronic communication" from the power company that electronic payments were no longer being accepted and to send a check by mail - so the bank sent out a check.

When the electric company did not receive the check, the business had its power cut. The business owner then authorized another payment to the electric company over the phone, assuming the check would reach the company at a later date and would be applied as credit to their account for their next bill. However, the business owner received another notification about an upcoming payment the following month.

The check was never received, and no credit was posted to the account.

RUNNING SHORT ON TIME

We needed to act fast. The business owner who was targeted could be revictimized, and the individuals involved could move states, change their names, or otherwise attempt to evade detection. This would leave them free to target other business owners. Within ~48 hours, we had to determine who exactly was involved, where they were located, and how they were connected. Within that timeframe, I had to compile information on the suspects and draft a police report in a way that makes things obvious and easy to understand for law enforcement. Time was ticking.

WHAT ARE WE DEALING WITH?

1. Phishing, or an internal bad actor?
2. Check-washing, or counterfeiting?
3. Who are the people involved?
4. How many people are involved?

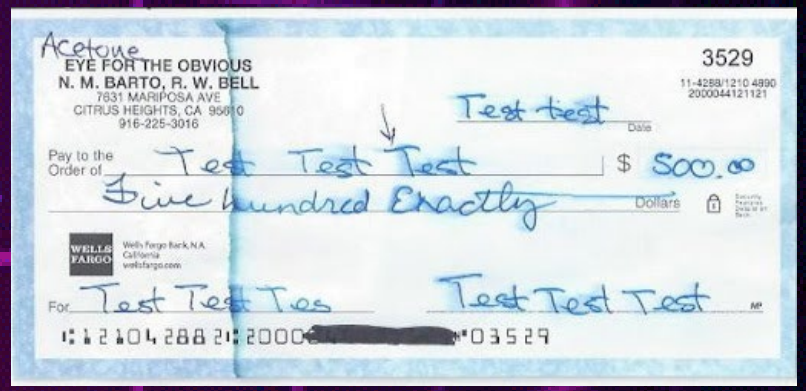
PHISHING

Phishing is not a new social-engineering tactic, and most companies train their employees against phishing attacks. While it is very possible that a phishing attack fooled a bank employee, it could also be an insider working at the bank who used an “email from the electric company” as an excuse or cover up for knowingly creating the counterfeit check.

We ***haven’t seen*** proof of the “electronic communication” from the electric company that was sent to the bank ourselves. Another employee at the bank confirmed that there was a note in the business owner’s account regarding electronic communication received from the electric company.

Was there a phishing email or was that just a cover story?

DIGITAL CHECK WASHING VS COUNTERFEIT



We determined that this wasn't a case of check-washing. According to the bank, checks that are authorized through the bank's app are sent from a location in Evanston, Indiana. If the check was originally addressed to the electric company, it would have been en route from Evanston to the company's office in Chicago. Yet, the check was addressed to an individual in Rantoul, and cashed in Danville. It would be unusual for a check originally from Evanston, Indiana en route to Chicago, Illinois (a northwest route) to be intercepted in Rantoul, located further southwest. This would require one to divert from the original route, and such a detour would add significant time.

More importantly, the check was intentionally and originally made out to an individual (not the electric company), this was apparent on the copy of the check that was included in the business owner's account history. Therefore, we concluded that we were looking at a case of counterfeit.

NOT EXACTLY CRIMINAL MASTERMINDS

You'd think he'd have learned by now...

A counterfeit check was created and sent by an unknown bank employee, not to the electric company, but to an individual located in Rantoul, who then *signed it over* to another individual in Danville to be cashed.

These individuals used their full legal names, and a copy of the check was saved to the business owner's bank account, showing exactly who the check was addressed to.

A quick people-search engine inquiry led us straight to their personal information, social media profiles, and current addresses. The individuals involved were *even friends on social media*. The main suspect has a long criminal history, with public court records dating as far back as 1993 to as recent as 2022 revealing that the man is an armed habitual criminal.

His crimes include a history of domestic abuse, assault, burglary, theft, counterfeiting, possession of methamphetamine, and **previous counts of forgery and fraud**. He's even been featured in local news more than once. He just keeps getting let off easy.

HOW'D THEY CHOOSE THEIR TARGET?

The main criminal involved had a mutual friend with the business owner on social media and suspect #2 who cashed the check was social media friends with an employee at the business owner's bank. While the owner is now aware of these "mutual friends" and their connection to the suspects, there's no telling who exactly was involved other than the two individuals who handled the check, why/how they chose the target, or if it there was a personal agenda behind the selection.

The **exact motive remains unclear**, *and we would need the bank's assistance* in determining the identity of the bank employee involved in the fraud, which we haven't received. There may be some level of internal involvement at the bank that should be a cause of concern for all individuals who have an account with that bank.

The criminal might not be a mastermind, but his actions have caused financial harm to a small business and left the victim worried for their personal safety.

FRAUD IMPACT ON SMALL BUSINESSES

- 2023 statistics from the Federal Trade Commission reported that consumers lost over $10 billion to fraud in 2023, a significant increase from the $3.3 billion reported loss in 2020. This increase includes significant amounts lost to investment scams ($4.6 billion) and imposter scams ($2.7 billion).

- Small businesses are frequent targets of these scams due to their perceived vulnerability and lower defenses compared to larger corporations. Financial strain from fraud can lead to operational challenges and, in severe cases, business closure.

- Association for Financial Professionals (AFP) Payments Fraud and Control Survey 2021: 51% percent of businesses indicated that after a successful fraud attempt, the organization was unable to recover funds lost. Almost two thirds of businesses recover 25% or less, and only one fourth recover more than 75 percent.

WE GOT HIM!

Thankfully, with the information I was able to find and put together in the report that was sent to police, the main bad actor was booked! We can only hope they give him a longer sentence.

[redacted] WAS BOOKED IN CHAMPAIGN COUNTY, ILLINOIS FOR FORGERY/POSSESS WITH INTENT.

Booking Number: [redacted]
Booking Date: 7/17/2024
Age: 45
Gender: M
Race: W
Height: 6 ft 02in(s)
Weight: 185 lbs
Hair Color: BRO
Eye Color: BRO
Arresting Agency: ILCHAMPAIGNSO

The lesson to this story is that it **doesn't take a lot to help your community**. If you're feeling stuck or discouraged with your OSINT skillset, or you've expanded on your skillset but haven't been able to put those new skills to use, I really want to let you know that even the most basic OSINT skills can really help somebody and make a difference in their lives.

Being able to help another small business owner meant a lot to me and it meant a lot to Natalie who has a family to support. Her business is her livelihood. Even being able to provide a detailed report to police is helpful when it comes to protecting her business.

OSINT RESOURCES: WHERE TO START

Remember to **weave a web** of information! Connect the threads.

1. People Search Sites

- https://www.truepeoplesearch.com/
- https://www.fastpeoplesearch.com/
- https://www.familysearch.org/en/united-states/

2. Public County Record Online Databases

3. Social Media Sites (Facebook, Instagram, etc)

4. Advanced Search Parameters/Google Dorking

5. Archive Sites

- https://web.archive.org/
- https://archive.ph/

REFERENCES

Federal Trade Commission. (2024, February). Nationwide fraud losses top $10 billion in 2023 as FTC steps up efforts to protect the public. https://www.ftc.gov/news-events/news/press-releases/2024/02/nationwide-fraud-losses-top-10-billion-2023-ftc-steps-efforts-protect-public

JPMorgan Chase & Co. (2021). 2021 AFP payments fraud and control survey report highlights. https://www.jpmorgan.com/content/dam/jpm/commercial-banking/documents/fraud-protection/2021-afp-payments-fraud-and-control-survey-report-highlights.pdf

Shorten, D. (2023, September 26). What every small business needs to know about fraud. PNC Bank. https://www.pnc.com/insights/small-business/manage-business-finances/what-every-small-business-needs-to-know-about-fraud.html#:~:text=The%20Association%20of%20Certified%20Fraud,control%2C%20and%20processes%20in%20place

CONTACT

EMAIL: TEUTHIDA@PROTON.ME

WEBSITE: SQUIDDLE.IO

MASTODON: DEFCON.SOCIAL/@TEUTHIDA

INSTAGRAM: 0XHEGEMON1C

TWITTER/X: @DYKEHERETIC

SHOP TIKTOK: 5QU1D3Y3