ECE458/ECE750T27: Computer Security

Threat Models and Risks

Dr. Kami Vaniea,
Electrical and Computer Engineering
kami.vaniea@uwaterloo.ca

UNIVERSITY OF WATERLOO | FACULTY OF ENGINEERING

Cybersecurity sometimes seems opposite to usability

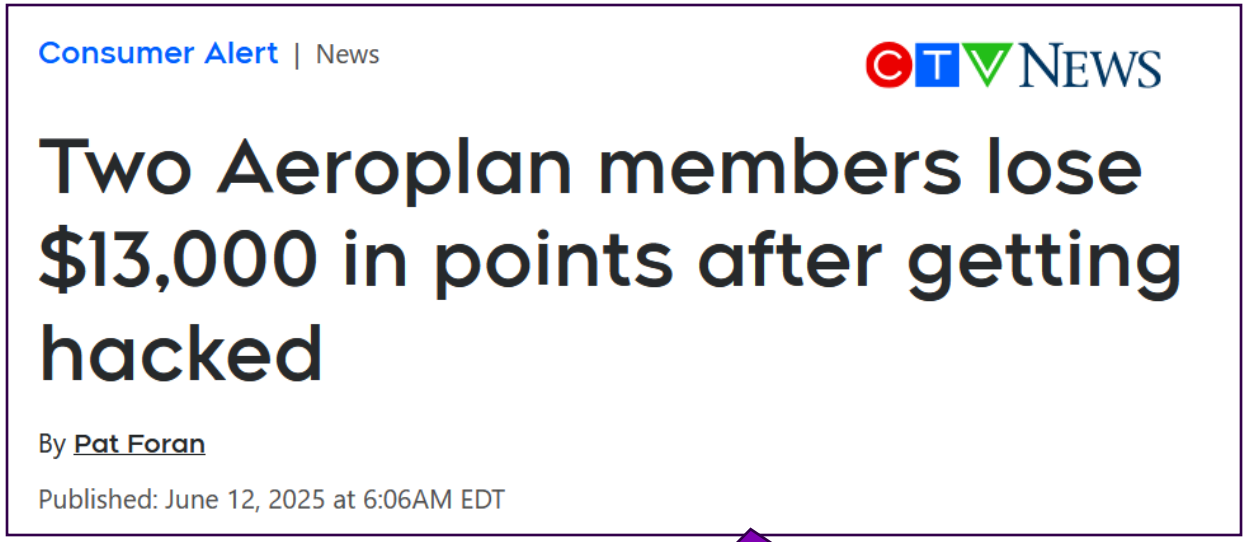
- Websites are amazing
  - **BUT DON'T CLICK ON THAT LINK!**
- Your phone can run all sorts of amazing apps for free
  - **BUT MANY OF YOUR APPS ARE EVIL!**
- AI is amazing and can do whatever you want
  - **DO NOT CONNECT AI TO ANYTHING IMPORTANT!**

"This World of Ours" by James Mickens in ;login: logout, January 2014

THREAT MODELS

Threat model

- Who is the adversary?
- What are their goals?
- What are their capabilities?
- What resources need protection?
- What risks can be accepted?



Consumer Alert | News

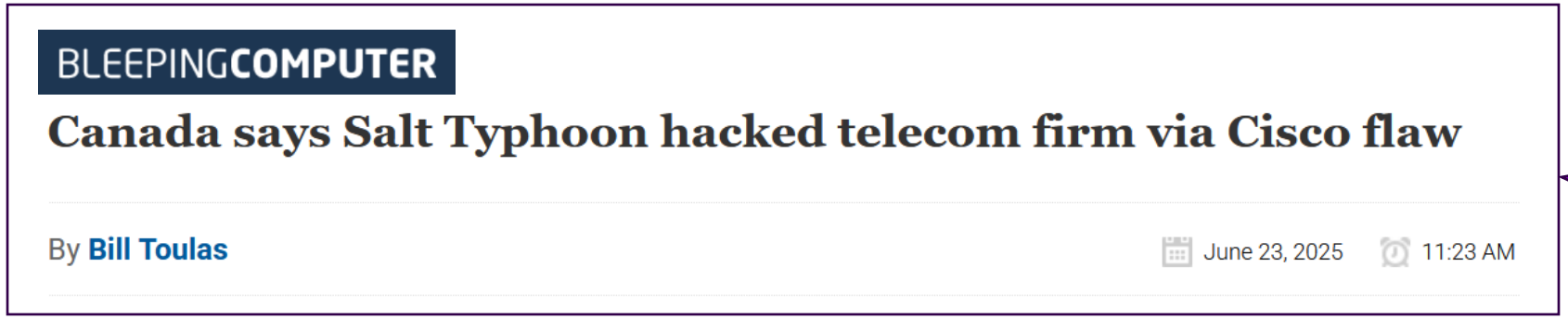
CTV NEWS

Two Aeroplan members lose $13,000 in points after getting hacked

By Pat Foran

Published: June 12, 2025 at 6:06AM EDT

Individual-level loss



BLEEPINGCOMPUTER

Canada says Salt Typhoon hacked telecom firm via Cisco flaw

By Bill Toulas

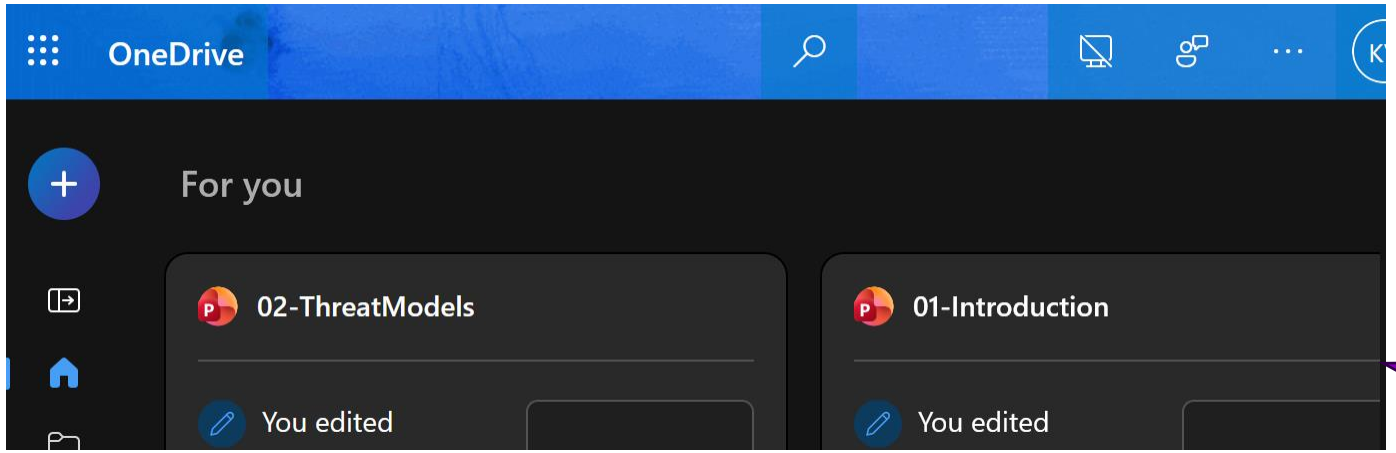
June 23, 2025 11:23 AM

Infrastructure hack of a country

Threat model

- Who is the adversary?
- What are their goals?
- What are their capabilities?
- What resources need protection?
- What risks can be accepted?

Wikipedia
"anyone can edit"



My OneDrive files

Who is the adversary?

- Government
- Criminal organization
- Individual attacker
- In-home threat
- Someone the user knows

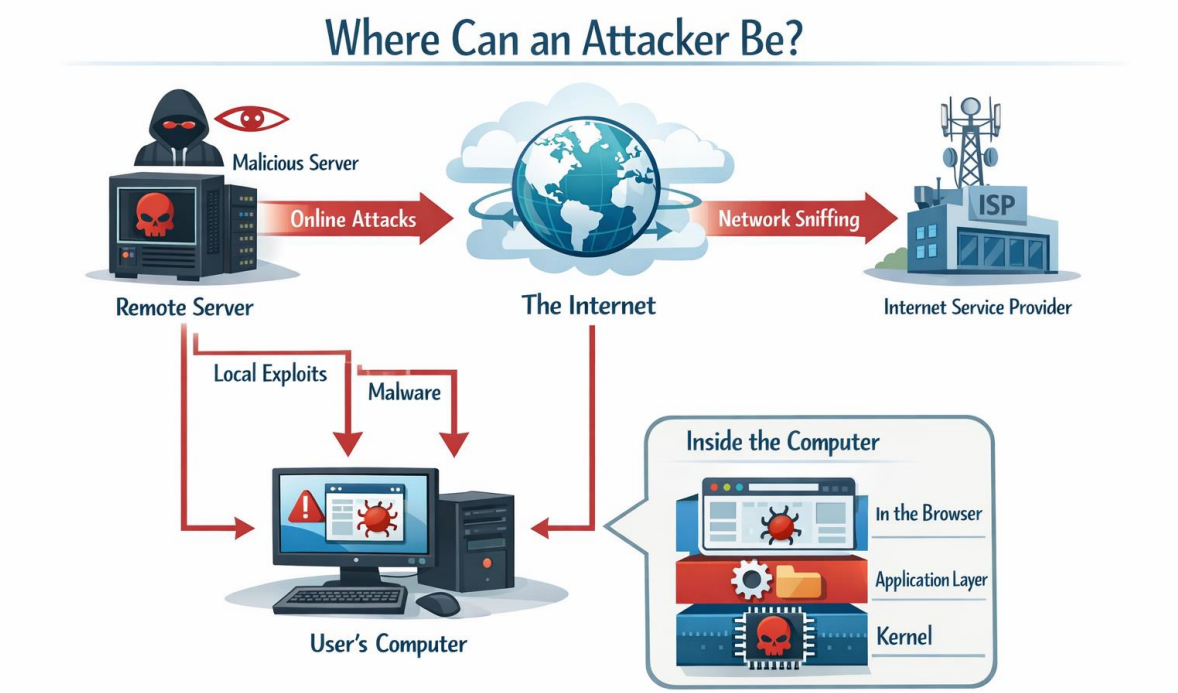
What are their goals?

- Steal data
- Steal money
- Prevent access
- Create inaccurate data
- Blame someone else for something

Security definition	
Confidentiality	No improper information gathering
Integrity	Data has not been (maliciously) altered
Availability	Data/services can be accessed as desired
Accountability	Actions are traceable to those responsible
Authentication	User or data origin accurately identifiable

What are their capabilities?

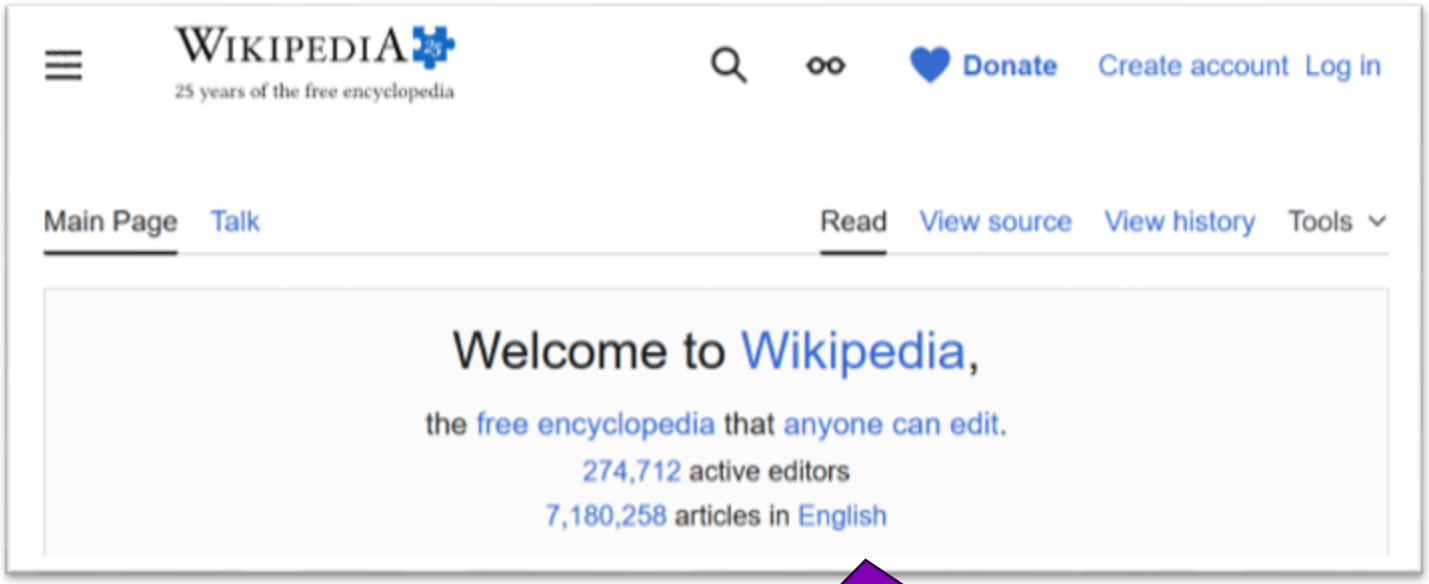
- Where is the attacker located?
  - Network
  - Remote server
  - Malicious software in a kernel
  - Compromised browser
  - In the home (physical access)
- What other capabilities?
  - Access to databases
  - Ability to cause physical impact



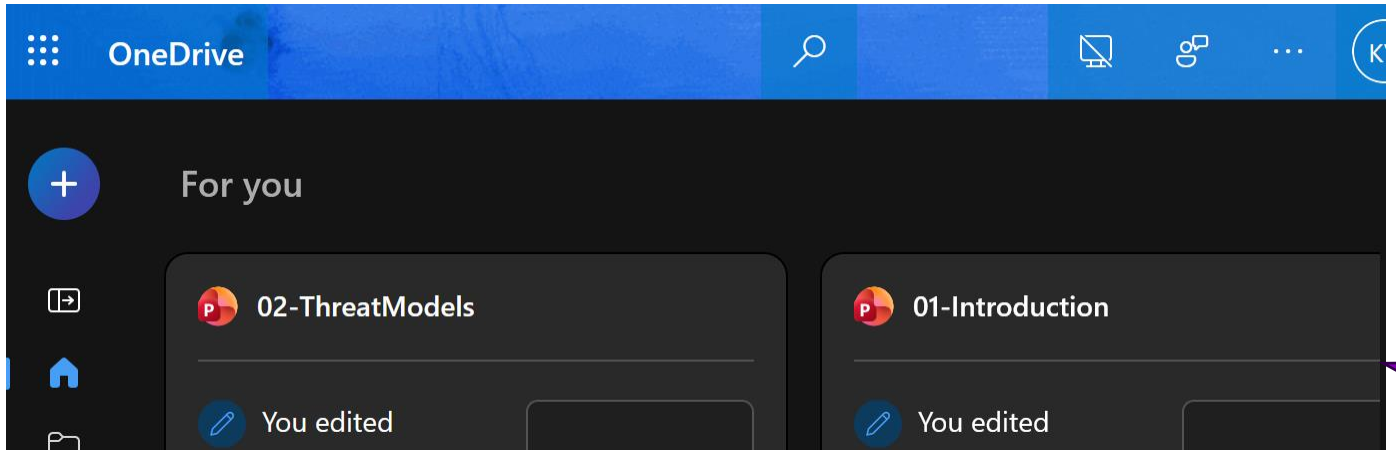
ChatGPT Generated

What resources need protection?

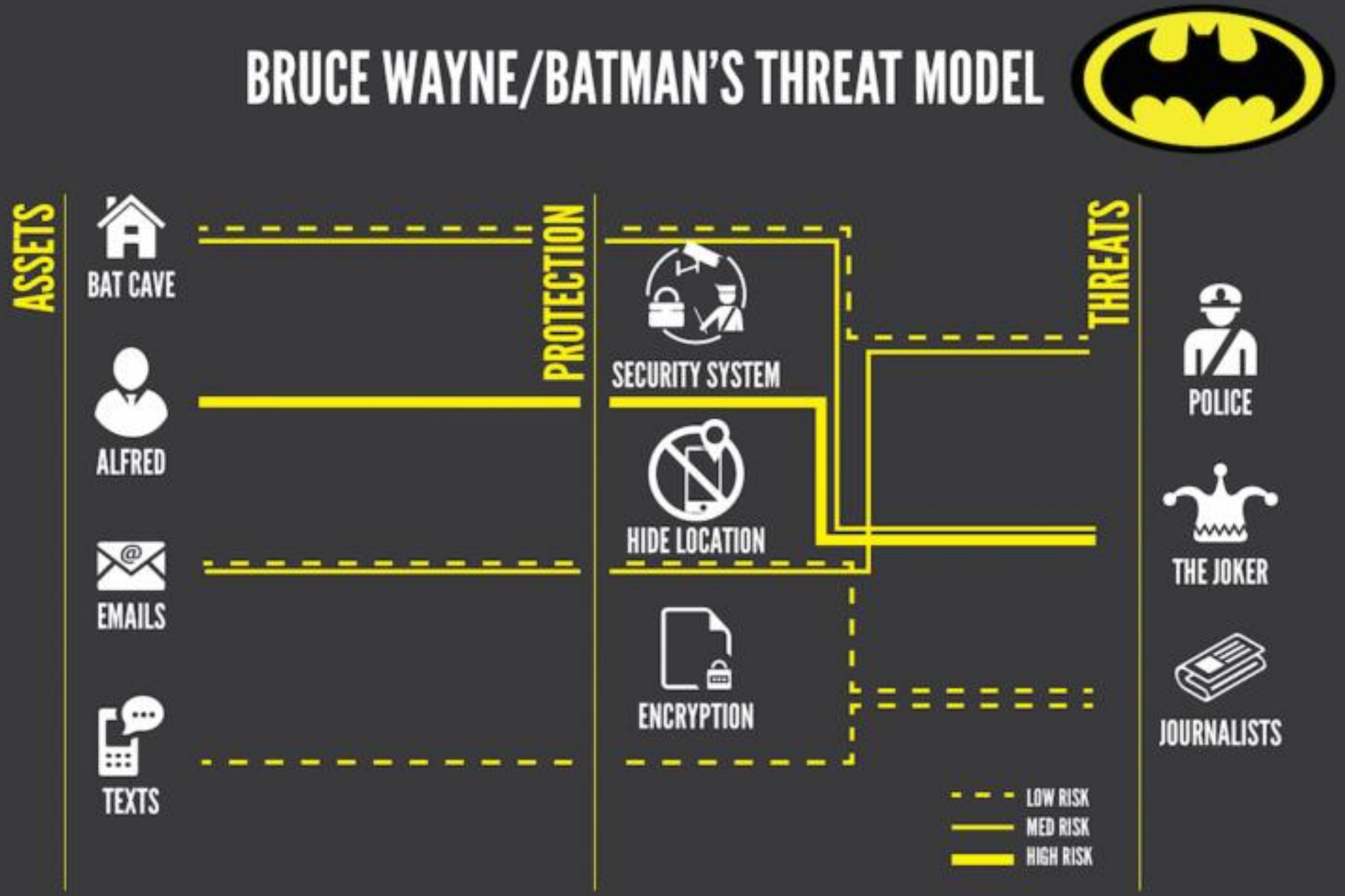
- What is valuable?
- What kinds of protection does it need (Confidentiality? Integrity?)



Wikipedia
"anyone can edit"



My OneDrive files



https://arstechnica.com/information-technology/2017/07/how-i-learned-to-stop-worrying-mostly-and-love-my-threat-model/

Risk acceptance

- All actions have risks, avoiding all risks is unrealistic
- What risks are you willing to accept
  - I might email the wrong file to the wrong person
  - Someone might guess my password
- How much are you willing to pay to avoid a risk
  - Double check the “from” field in every email
  - Have a 16 character random password

Investigative Journalist

University Professor

TECH SUPPORT SCAM EXAMPLE

Attacks have many aspects to them

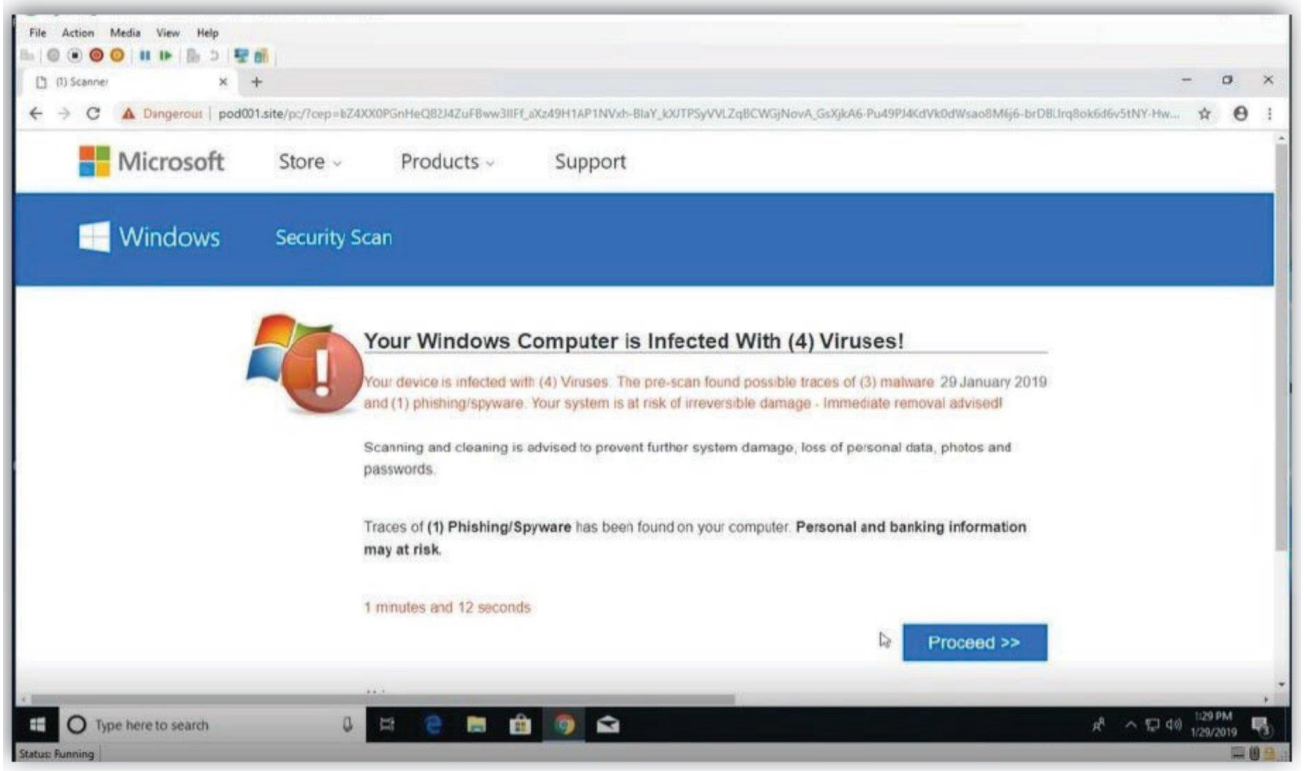
My points:

- Threats are not all classic attackers
- Attacks cross company boundaries
- Law enforcement is not the only threat to attackers
- Legit business can be attackers
- Doing the right thing can cost money
- Attackers must also protect themselves

- Think about:
  - Was there a hack?
  - Where is the money and who gets it?
  - What protections are being bypassed?
  - Can harmed groups do anything?
  - What is Tech Live's threat model?

Classic tech support scam: Tech Live Connect

- Users saw an ad or a pop-up claiming computer virus infection
- User asked to download scanning software which claimed lots of viruses found
- User instructed to call a phone number
- Tech support claimed to be Microsoft and requested payment to fix the problem
- User pays, fraudster makes money



Federal Trade Commission. Nexway complaint (2023). https://www.ftc.gov/system/files/ftc_gov/pdf/nexway-complaint.pdf

Chargebacks: Tech Live Connect

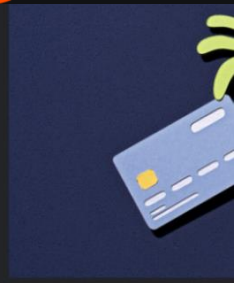
- Scheme relies on being able to process credit card payments
- Some users realized they had been scammed and filed a credit card chargeback
- Credit card processers know that if lots chargebacks occur often fraud is happening
- Companies with high rates of chargebacks get charged extra fees

ars TECHNICA

Your tech support company runs scams. Stop—or disguise with more fraud?

Fake it till you make it.

NATE ANDERSON – APR 13, 2026 3:58 PM | 64



Credit: Getty Images

Michael Cotter had a problem: "Chargebacks" at his tech support company were too high. The reason for this was not hard to find; people at his company, Tech Live Connect, were scamming Cotter's fellow Americans.

The scams usually began with a pop-up message warning that a user's computer might have a virus. The pop-up then claimed to run a "scan" (which was always positive) of the computer and provided a toll-free number to call for more help. Those who called were connected to Tech Live Connect's Indian call center, where they were asked for remote access to their computers, diagnosed with fake problems, and charged hundreds of dollars to "fix" them. Call center workers often pretended to be Apple or Microsoft employees.

Defrauded people complained in droves.

Even worse—they filed chargebacks with their credit card companies, disputing these payments. A high rate of chargebacks is usually a pretty good sign of fraud, and payment processors will often apply penalties or stop credit card acceptance altogether if chargeback ratios climb too high. By the middle of 2015, one payment processor was already warning that it could soon terminate five of Tech Live Connect's merchant accounts over chargeback concerns.

To make the problem stop, Cotter could have clamped down on the fraud, of course, but this was where the money was. Cotter did claim that he had a policy of firing call center workers who conducted scams, but he eventually admitted that the policy "was not enforced consistently." Repeat scammers at his company were in some cases promoted, not fired.

Scam payment processor

- Tech Live Connect started buying debit cards, then charging those cards as if they were customer cards thereby reducing the chargeback rate
- Most transactions have processing fees, so Tech Live Connect was lost nearly half the money they used to pay themselves

Rhode Island Man Sentenced for Years-Long Bank Fraud Conspiracy

Friday, April 10, 2026

Share

Office of Public Affairs
U.S. Department of Justice

For Immediate Release

Office of Public Affairs

A Rhode Island man was sentenced yesterday to 28 months in prison for deceiving banks by artificially inflating his company's sales numbers to avoid bank scrutiny over its excessive consumer chargebacks.

According to court documents, Michael Brian Cotter, 64, of Greenville, Rhode Island, was CEO of a tech support company that operated from a call center in India. In 2016, when banks began restricting the company's ability to process debit and credit card payments because of fraud and chargeback concerns, Cotter and his co-conspirators began purchasing virtual debit cards to run thousands of sham transactions on their own merchant accounts. In doing so, Cotter artificially inflated the company's sales numbers to make it appear to banks and their agents that the company's chargeback ratios — a key metric used by banks to detect fraud — were within acceptable levels. Although this tactic amounted to the company effectively paying itself, Cotter used actual customer personal identifying information, without customers' knowledge or consent, to disguise the transactions from banks by making them appear like legitimate sales.

Cotter pleaded guilty to conspiracy to commit bank fraud.

Assistant Attorney General A. Tysen Duva of the Justice Department's Criminal Division and Inspector in Charge Eric Shen of the United States Postal Inspection Service Criminal Investigations Group (USPIS CIG) made the announcement.

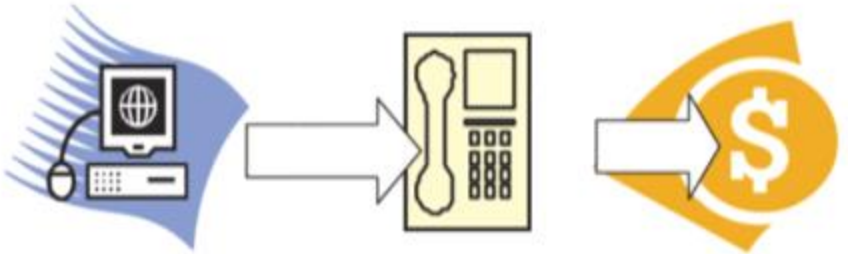
The USPIS investigated the case.

Trial Attorneys Jason Feldman and Shana Priore of the Criminal Division's Fraud Section prosecuted the case.

Updated April 10, 2026

Nexway processed Tech Live payments

- Tech Live Connect also contracted with Nexway to do payment processing using Nexway's accounts – they had a legal contract



Consumer (1) receives a deceptive pop up on his or her computer directing the consumer to call a number which leads to a telemarketer or (2) calls to activate software which leads to a telemarketer.

Telemarketer at call center deceptively pitches tech support services and charges consumers.

Nexway uses its merchant account to cause an acquirer to submit charges into the credit card system, collects money from consumers, and after taking a share, transfers the funds to companies scamming consumers.

From the FTC complaint

21. Ordinarily, sellers must obtain merchant accounts to process consumer credit card payments for the seller's good or services. By using its own merchant account to process consumer payments for third parties, Nexway made it possible for its clients engaged in tech support scams to obtain furtive access to the credit card system and evade detection by the card brands for a longer period of time. The charges Nexway surreptitiously placed in the credit card system and the collection of money consumers paid is the life-blood of tech support scams.

Federal Trade Commission. Nexway complaint (2023). https://www.ftc.gov/system/files/ftc_gov/pdf/nexway-complaint.pdf

How they were caught: consumer complaints

- Microsoft notified the Transnational Elder Fraud Strike Force
- Postal Inspection Service initiated an investigation

District Court Enters Permanent Injunction Shutting Down Technical-Support Fraud Scheme

Tuesday, December 29, 2020

Archives
U.S. Department of Justice

For Immediate Release
Office of Public Affairs

A federal court entered an order of permanent injunction against an individual and five companies in a case against a large-scale technical-support fraud scheme alleged to have defrauded hundreds of elderly and vulnerable U.S. victims, the Department of Justice announced today.

The order bars Michael Brian Cotter, 59, of Glendale, California, and four companies — Singapore registered Global Digital Concierge Pte. Ltd., formerly known as Tech Live Connect Pte. Ltd., Nevada registered companies Sensei Ventures Incorporated and NE Labs Inc., New York registered KeviSoft LLC — from selling technical-support services or software via telemarketing or websites.

"The department is committed to protecting vulnerable Americans, particularly America's seniors, from those who seek to steal their hard earned savings," said Acting Assistant Attorney General Jeffrey Bossert Clark for the Civil Division. "The department is grateful for the cooperation of foreign law enforcement, including India's Central Bureau of Investigation, in investigating, disrupting, and prosecuting technical-support fraud schemes and other schemes originating abroad and directed at the American public."

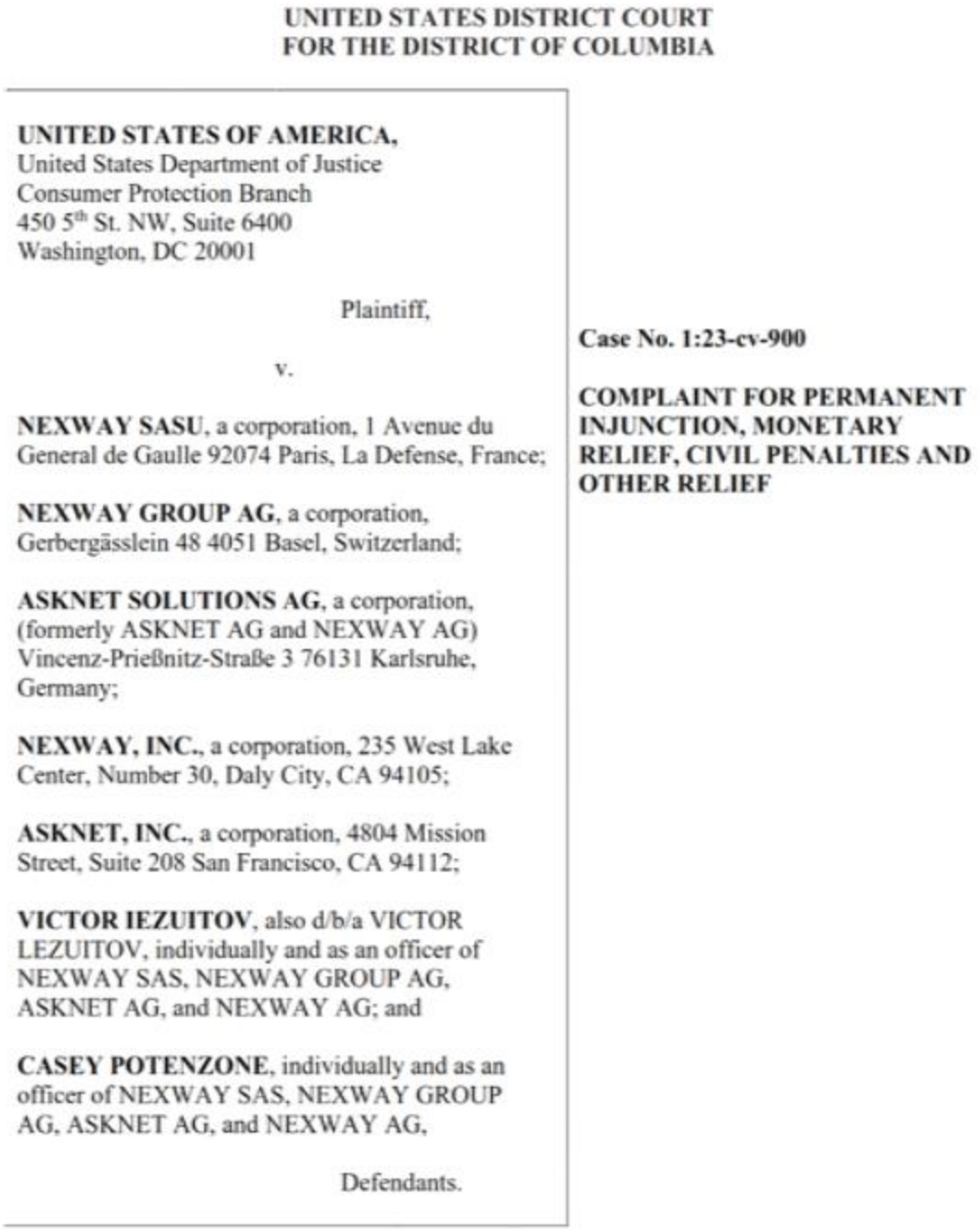
"The Postal Inspection Service is committed to investigating all types of elder fraud," said Damon Wood, Inspector in Charge of the Philadelphia Division of the U.S. Postal Inspection Service. "Fraudsters who scam the elderly and others online use fear and pressure tactics to prey on our most vulnerable Americans from the safety of a computer screen. The Inspection Service is proud of our domestic and international partners who extended the reach of our investigative efforts, shutting this scam down once and for all, and protecting American citizens."

The complaint filed in October 2020 alleged that Cotter worked with co-conspirators in India from at least 2011 to 2020 to operate a technical-support fraud scheme. The scheme allegedly contacted U.S. consumers via internet pop-up messages that falsely appeared to be security alerts from Microsoft or another well-known company. The pop-up messages fraudulently claimed that the consumer's computer was infected by a virus, purported to run a scan of the consumer's computer, falsely confirmed the presence of a virus and malware, and then provided a toll-free number to call for assistance. When victims called the toll-free number, they were connected to India-based call centers participating in the fraud scheme. Call center workers asked victims to give them remote access to their computers and told victims that they detected viruses or other malware on their computers. Eventually, the call center workers would falsely diagnose non-existent problems and ask victims to pay hundreds of dollars for unnecessary services and software.

US gov vs. Nexway

- Nexway was prosecuted for enabling the tech support scam
- Key in the decision is that Nexway knew Tech Live Connect was scamming people

> Since in or around August 2016, Nexway knew or consciously avoided knowing that its client, Tech Live Connect, and other foreign tech support call centers clients, made false or misleading statements to induce consumers to pay for purported tech support services. Yet, Nexway continued to illegally process Tech Live Connect's unlawful charges through its merchant accounts until at least February 2020.



UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

UNITED STATES OF AMERICA,
United States Department of Justice
Consumer Protection Branch
450 5th St. NW, Suite 6400
Washington, DC 20001

Plaintiff,

v.

NEXWAY SASU, a corporation, 1 Avenue du General de Gaulle 92074 Paris, La Defense, France;

NEXWAY GROUP AG, a corporation, Gerbergässlein 48 4051 Basel, Switzerland;

ASKNET SOLUTIONS AG, a corporation, (formerly ASKNET AG and NEXWAY AG) Vincenz-Prießnitz-Straße 3 76131 Karlsruhe, Germany;

NEXWAY, INC., a corporation, 235 West Lake Center, Number 30, Daly City, CA 94105;

ASKNET, INC., a corporation, 4804 Mission Street, Suite 208 San Francisco, CA 94112;

VICTOR IEZUITOV, also d/b/a VICTOR LEZUITOV, individually and as an officer of NEXWAY SAS, NEXWAY GROUP AG, ASKNET AG, and NEXWAY AG; and

CASEY POTENZONE, individually and as an officer of NEXWAY SAS, NEXWAY GROUP AG, ASKNET AG, and NEXWAY AG,

Defendants.

Case No. 1:23-cv-900

COMPLAINT FOR PERMANENT INJUNCTION, MONETARY RELIEF, CIVIL PENALTIES AND OTHER RELIEF

Federal Trade Commission. Nexway complaint (2023). https://www.ftc.gov/system/files/ftc_gov/pdf/nexway-complaint.pdf

Think about:

- Was there a hack?
- Where is the money and who gets it?
- What protections are being bypassed?
- Can harmed groups do anything?
- What is Tech Live's threat model?

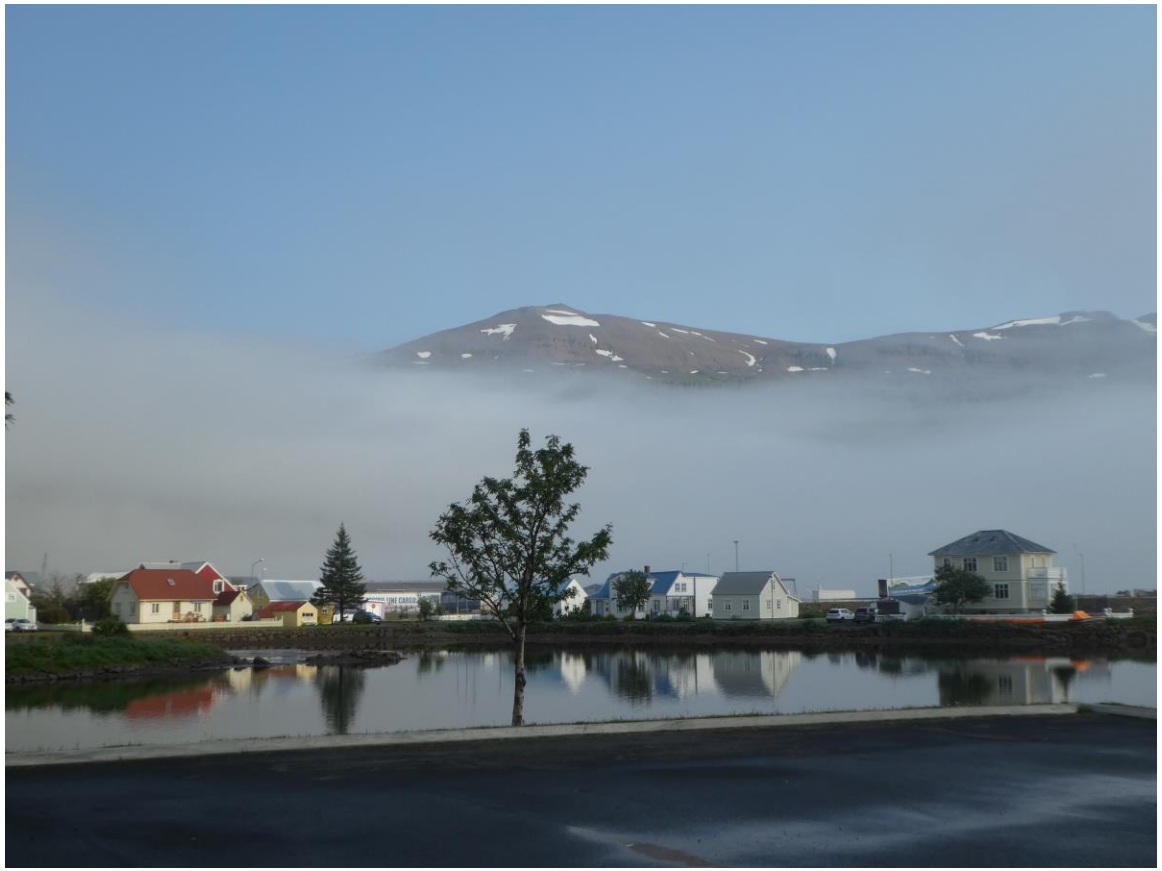
PHILOSOPHICAL APPROACH TO SECURITY

Philosophical approach to security

- Military approach to security is like a castle
  - Entrance is guarded by skilled professionals
  - Entities inside the castle are allowed because they were verified at the gate
  - Security inside each section is minimal

Philosophical approach to security

- Or should security be more like a village that is open to entry
  - Each house has its own locks
  - Each home owner decides their security level
  - Security detection is done by all residents
  - Non-security people are less good at security



Questions