CS 573 Midterm Project

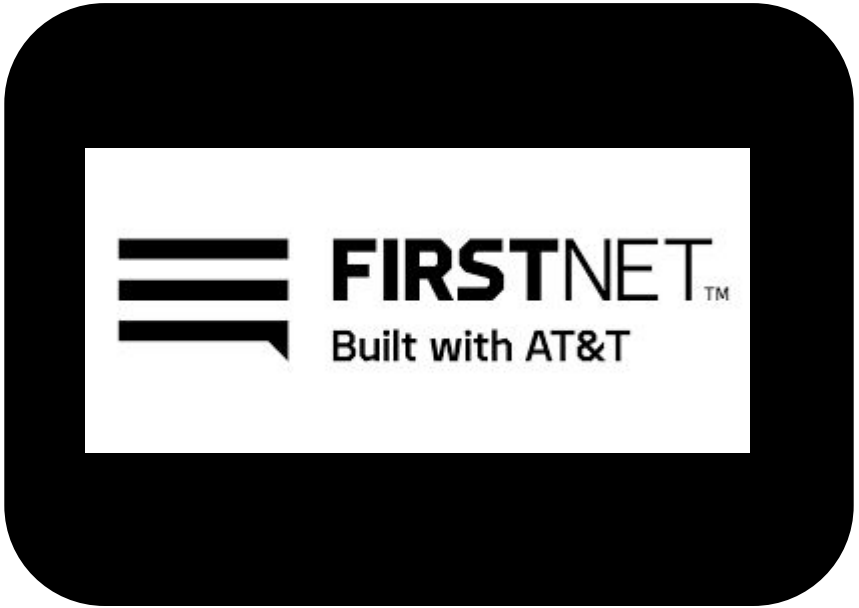
Anjali Gupta

"I pledge my honor that I have abided by the Stevens Honor System"

AT&T - Attack

“FirstNet admin network hacked due to AT&T Cybersecurity Engineer/Tester having testing credentials on an excel spreadsheet. Hacker was able to get into employee’s computer and view the spreadsheets but not other password protected web applications.”

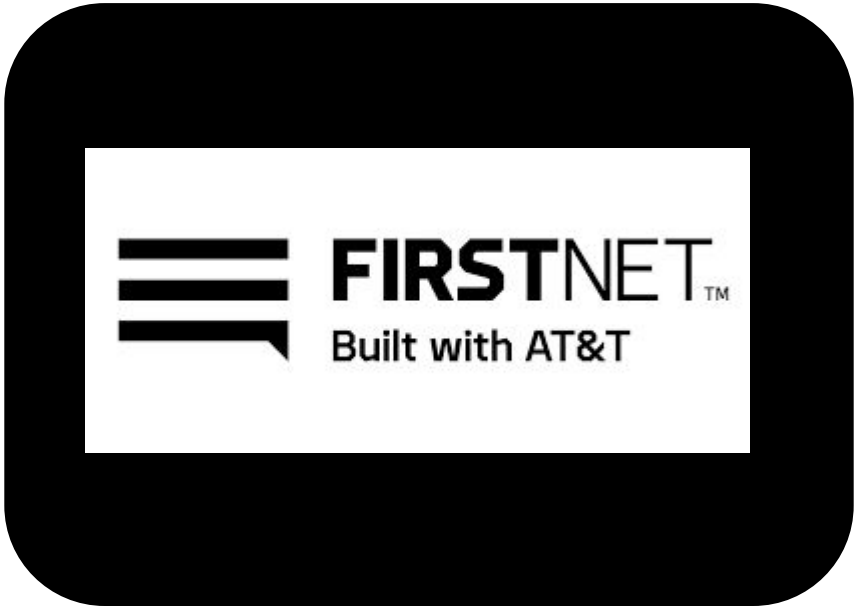
Date: February 2026



AT&T - Prevention

Utilize password protected spreadsheets

Use a password vault to make sure credentials are not easily accessible in cases where a computer may become compromised.



FBI - Attack

“Foreign adversary admits to data scraping FBI records in the 30 seconds before session timeout after employee access. Data is being possibly used to train AI deepfake models and impersonations. ”

Date: January 2026

FBI - Prevention

Should have banned IP address when first suspicion of data scraping activity occurred.

Enforce immediate employee logout from systems rather than just allowing it to timeout.

New York PD - Attack

“NYPD IT department victim of AitM phish, allowing hackers to bypass 2FA measures issued by system. 50 two-step verification tokens stolen from employees, credentials posted on dark web.”

Date: January 2026

New York PB - Prevention

Use of stronger MFA authorization rather than just a simple 2FA token

Use of biometrics such as fingerprints or retina scan.

Can use YubiKeys or something of that equivalent

Employee training on identifying phish emails.

Walmart - Attack

“Walmart IT administration become victims of ‘pass-the-cookie’ attack (verification cookies stolen from user and hacker is able to bypass MFA) on third party Microsoft Azure management portal. Hacker is then able to replace the entire Walmart.com interface with stock image of a cat.”

Date: June 2025

Walmart - Prevention

Have a system where a cookie generated by a user is stored in a database as being used with a specific IP address, once the session is over, database should mark the cookie as used.

If someone else is trying to use that cookie (either a used cookie or a cookie from a different IP), it will be unable to authenticate the user.

Meta - Attack

“Deepfakes and AI generated fakes news of political Cory Booker swarm Meta platforms amid midterm elections, Meta employees unable to find source of posts. Posts were not taken down immediately over hesitation regarding first amendment legislation”

Date: September 2026

Meta - Prevention

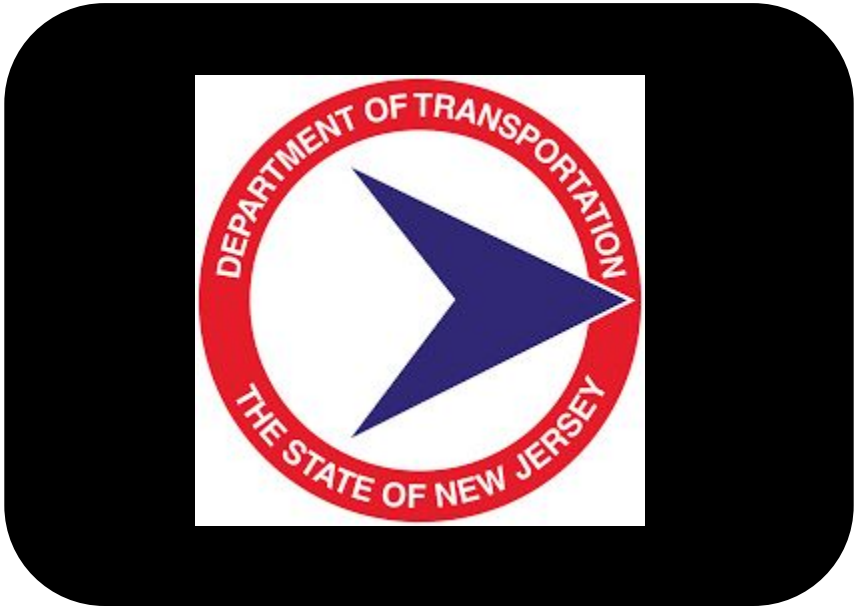
Proper legislation/guidelines put in place that state how social media platforms should deal with deepfakes and AI generated content.

National law and hold social media platforms responsible (Meta, LinkedIn, Tiktok etc.)

NJDOT - Attack

“Files from NJDOT Oracle database containing bridge and tunnel information found on the dark web. Information was posted by a bribed NJDOT employee who had access to database and sold for $100,000 to hackers.”

Date: November 2025

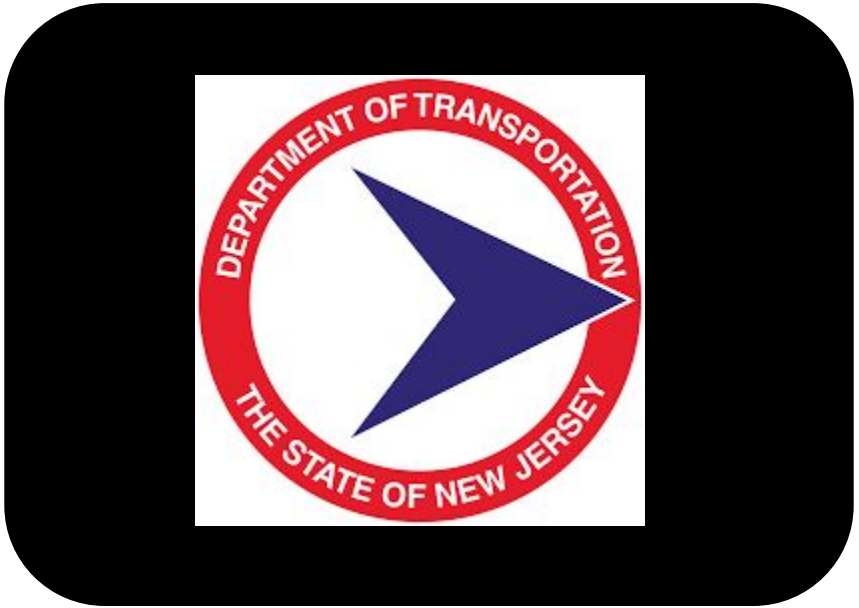


NJDOT - Prevention

Ensuring authorization hierarchy (who can access the data, what level of data they can access)

Limit access to specific data sets.
Use keystroke logging or recorded access sessions for sensitive data to ensure no one is stealing or downloading data sets

Immediate logout after very short periods of inactivity, especially with sensitive data



Uber - Attack

“100,000 Uber drivers do not receive ‘instant payments’ from a full day of earnings due to a third party service (Stripe) hack of the payment processing system. Hack done by stealing authentication cookies from a Stripe admin account.

Date: October 2025

Uber - Prevention

Put authentication cookies into a database and mark them as used when admin is done with the session to ensure hackers can not reuse authentication cookies.

Cricket Wireless - Attack

“Hackers compromise 5,000 Cricket wireless using the ‘reset password’ function on user login. Hackers then sent socially engineered personal messages to request codes sent to user’s phones. 5,000 users sent codes to hackers unknowingly, accounts compromised.”

Date: March 2026

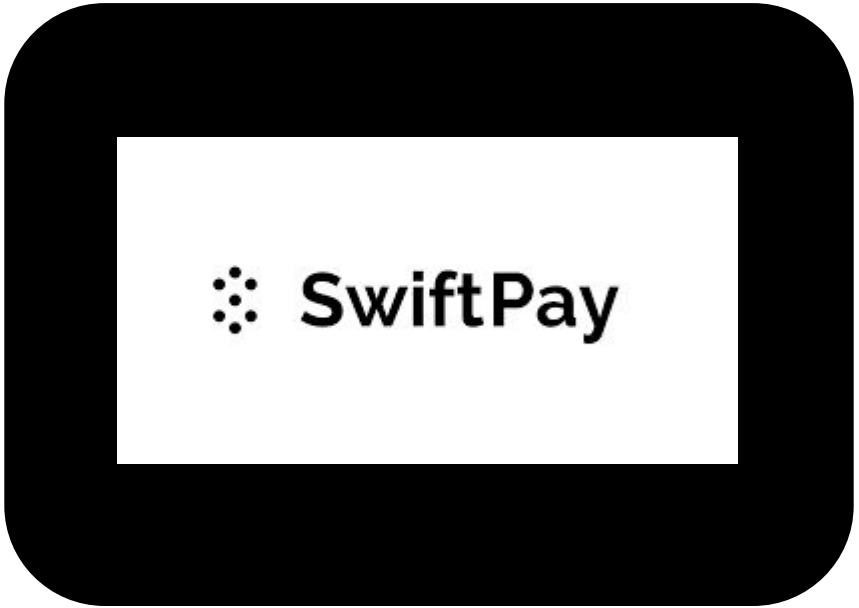
Cricket Wireless - Prevention

Have an OTP system authenticator on a user;s phone (such as Microsoft authenticator) synced to a Cricket accounts in case of ‘forgotten password’ problems. That way a user isn’t relying on an SMS sent from the company
Completely shift from passwords and use biometrics as MFA

SwiftPay - Attack

“Hacker uses credential stuffing to gain access into SwiftPay Merchant Portal accounts and change primary email to a temporary email using Yopmail. Hackers then link a new bank account to drain money from the user’s account”

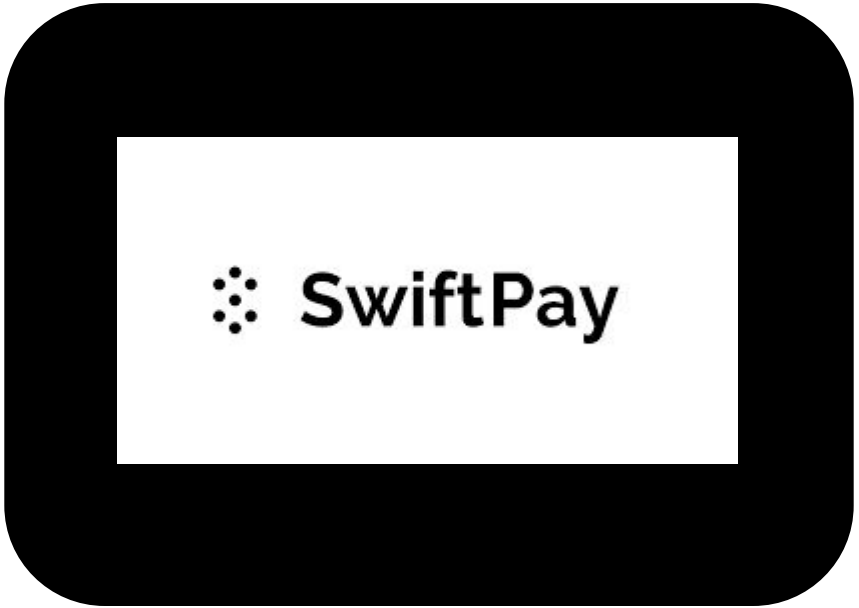
Date: August 2025



SwiftPay - Prevention

Creating a system that can detect the usage of a temporary email address/prevent users from using temporary email addresses for their accounts.

Prevent the changing of email addresses from “valid” domains to temporary domains



Target - Attack

“Hackers use AI generated messages and graphics to launch phishing attack against Target IT administrators. Believed that DeepSeek’s latest model was used to generate messages and graphics. Hacker inputted personal and professional information regarding top IT officials into DeepSeek and gave personalized phishing emails to each administrator. Some phish emails included deepfakes of higher administration.
Date: January 2026

Target - Prevention

Use of a AI/ML system to detect AI generated emails/graphics which will indicate it likely stemmed from outside of the administration system.

Similarly, use an AI model that has been trained on phish emails and can therefore detect phishing emails.

TD Bank - Attack

“TB Banking becomes infected with botnets. Hackers used malware-as-a-service (MaaS) platforms (most likely RedLine), replicas of SaaS cloud platforms, from the dark web to extract login credentials and credit card information from already infected/compromised web pages. Credentials and banking information held for ransom where TB Bank users paid up to $10,000 each in retrieving their information.”
Date: December 2025

TD Bank - Prevention

Patch management by hiring ethical hackers to find gaping holes within the system and then patch

Implementing an AI/ML malware detection system to detect malware faster, autonomously and without human delay.

ChatGPT - Attack

“Hacker uses credential stuffing to log into ChatGPT accounts. Hacker is then able to use simple prompts such as ‘Tell me everything you know about me’ and extract information such as university of attendance, age, hometown etc. Hacker then stalks 20 students on the Stevens Institute of Technology campus, restraining order put into place.”

Date: June 2025

ChatGPT - Prevention

Provide ways/information for users on how to clear the data they have inputted into the model

Encourage users to not use personal information when interacting with GPT

Remind users to clear data at the end of every session to prevent hackers from stealing input data

ActBlue - Attack

“Amid midterm elections, Rhode Island Senator incumbent Jack Reed’s campaign team victim of a phishing attack in which $500,000 dollars worth of campaign donations stolen via ActBlue platform. Released a statement stating one of campaign managers was victim of phish which installed pirated software onto their computer. Foreign adversary was able to view the computer screen, take login credentials, remove 2FA and drain account.”

Date: September 2026

ActBlue - Prevention

Employee training on phishing and being wary of suspicious emails, especially when there are grammatical errors and foreign email domains.

Up-to-date anti-malware software installed, especially as a political candidate.

Have a dedicated cyber team (1-2 people) to ensure proper course of action.

Waymo - Attack

“Waymo navigation system down due to jamming attack: disruption of satellite signals, preventing GPS from knowing its location) by foreign adversary. Waymo cars down in Los Angeles and New York. Due to Waymo system, cars in New York stopped in the middle of streets causing severe traffic jams.”

Date: August 2025

Waymo - Prevention

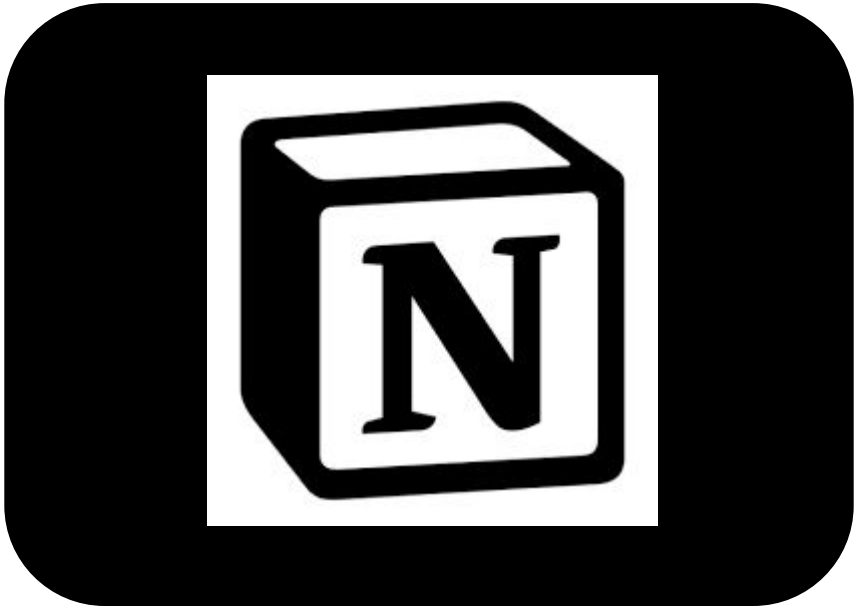
Implementation of a GPS jamming detection system.

Utilize smartphone-based networks to provide timely alerts and indicators on potential jamming.

Notion - Attack

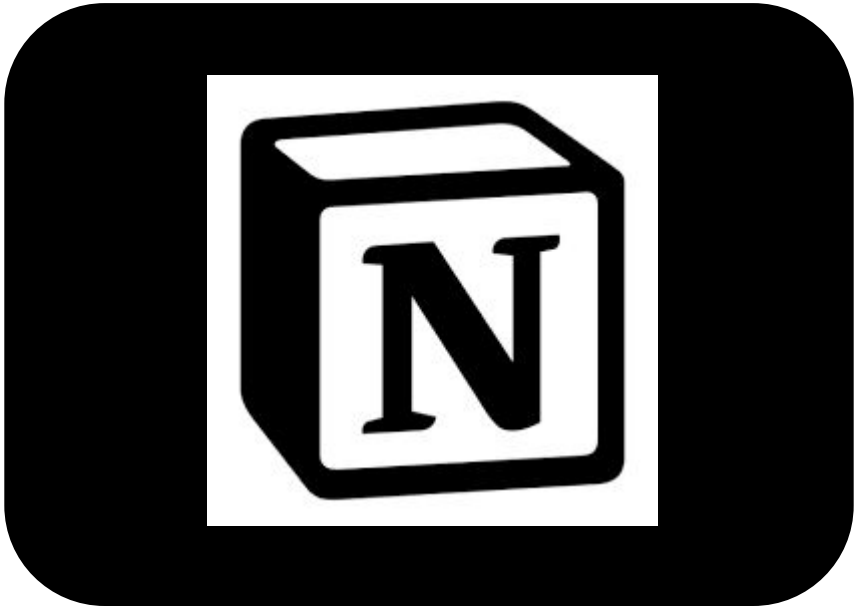
“Hacker uses SQL injection technique (when asked for password) on web login page and is able to receive the full database on user accounts and information. Over 100,000 accounts compromised.”

Date: June 2025



Notion - Prevention

Implement WAF (Web application firewalls) which basically protect web applications by monitoring traffic between web apps and the internet.



Pfizer - Attack

“Hacker able to manipulate new Pfizer AI model to release over 1 million patient data and records that was used as training data for LLM. Records had not been properly stripped of personally identifiable data. Records leaked onto Haystack on the dark web. Researchers calling this a case of a Leaky Language Model.”

Date: September 2026

Pfizer - Prevention

Proper encryption of patient data.

Ensure patient data has been stripped of any personally identifiable information.

Test model with popular prompts that have been used to manipulate LLM's in the past.

Spycloud - Attack

“Spycloud’s ‘Cybercrime Analytics Engine’, which is used to collect data from the darkweb and filter it based on value, subjected to ransomware attack. Company pays $15 million. Employee unknowingly downloaded files believed to be sent from his boss.”

Date: August 2025

Spycloud - Prevention

Building a continuity plan - what to do when your biggest asset is compromised.

AI/ML system for detecting phish emails.

Employee training on phishing (even as a cybersecurity company)

SIT - Attack

“Hacker uses credential stuffing, accessed from the dark web, to gain access into 100 Stevens undergrad accounts that did not have 2FA. Students had not updated passwords since summer before their first year. Posted grades from Workday onto Fizz.”

Date: April 2025

SIT - Prevention

Make students change passwords at the beginning of each academic year.

Passwords of 10-15 characters in length with a mix of special characters.

Barclays - Attack

“Barclays online web banking system subjected to DDOS attack, bringing the entire system down for over 24 hours. Suspicious activity seen as early as 5 hours before the attack, but was deemed normal and was dismissed. CISO apologizes and steps down.”

Date: July 2025

Barclays - Prevention

Early detection; if suspicious activity was seen that early, something should have been done about it.

Use of dynamic load balancing to spread traffic across different servers rather than select few being overloaded.

Outfront Media - Attack

“Outfront Media, one of the billboard companies in Times Square, is hacked with a deepfake of President Trump calling on young men to enlist in the army to go to war with Russia. Deepfake was on billboards for 30 minutes before it was taken down.”

Date: March 2026

Outfront Media - Prevention

Utilize AI to detect unauthorized uploads.

Use deepfake detection AI such as Deepware that are integrated into the system to stop those kind of uploads.

Enable biometric MFA (retina, fingerprint) to get access into system.

Amazon - Attack

“Hackers are able to get into 20 Amazon echo devices of top ranking Trump administration through the infiltration of home networks through ARP spoofing (allowing all traffic between the internet and IoT device to go through the hacker) 100 hours worth of conversations recorded, some with classified information. Conversations sold to newspaper outlets such as New York Times and the Washington Post.”

Date: April 2025

Amazon - Prevention

Enable mute function on echo device which disable the automatic listening.

Have VPN installed in home network to encrypt traffic.

Trump administration - Attack

“Guess they didn’t learn the first time… Leading Trump official, John Radcliffe messages assistant classified information regarding the ongoing Russia-Ukraine war from personal phone because he could not access his work email due to ‘temporary lockout’. China is able to decrypt the end-to-end encryption of message and post it on X.”

Date: November 2025

Trump administration - Prevention

Don’t be an idiot…for the second time in a row.

Use phone call to relay information rather than messaging.

Adhere to proper protocol regarding lockouts, utilize some form of password manager (preferably physical) to manage passwords.

LinkedIn - Attack

“Desperate college students become victims of DNS spoofing attack via an unassuming video call link interview link. Hacker made a fake LinkedIn account posing as a recruiter, reaching out to college students interested in internships. Video call link sent, once clicked, it injected false DNS information causing the redirection of the user to a phishing site.”

Date: September 2025

LinkedIn - Prevention

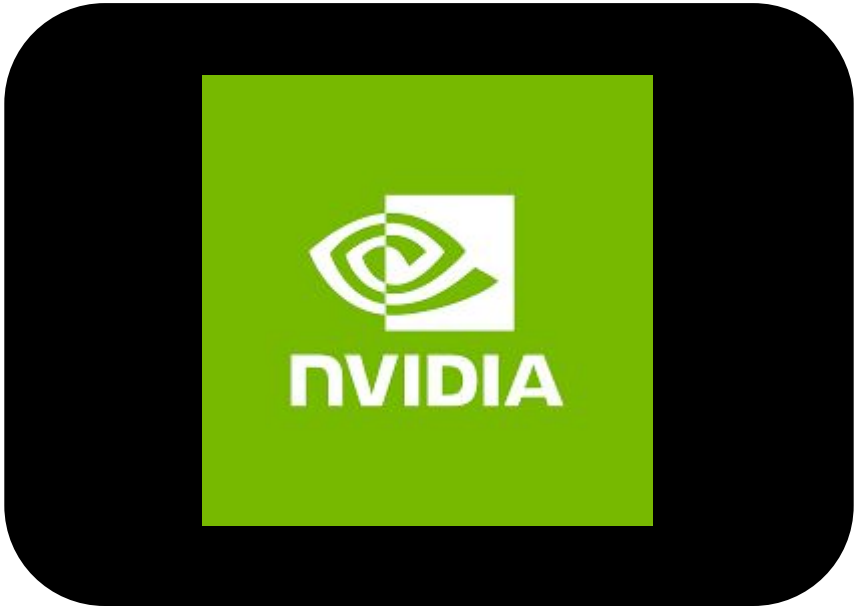
Encourage LinkedIn users to not directly click on links from LinkedIn direct messages. Give a secondary email to send a legitimate Microsoft Teams or Zoom link.

Check the validity of the company. Is it a legitimate company? Do they have a website and/or headquarters? etc.

Nvidia - Attack

“Nvidia robots given to various supermarket chains to implement ‘robot cashiers’ are exploited by hackers through an unpatched vulnerability. Hackers gain control of robots and make them do things such as attack patrons, knock over shelves, saying curse words, etc. Ended with physical shutdown by Nvidia employees.”

Date: August 2026



Nvidia - Prevention

Have some sort of behavior/audio detection system where the robot shuts down if it begins to say/do things that are “aggressive.”

Have on site personnel monitoring robots.