We'll get you there.

CPAs | CONSULTANTS | WEALTH ADVISORS

Securing the Mission: Cybersecurity for Nonprofits — Defending Good Deeds

June 26, 2025

The information herein has been provided by CliftonLarsonAllen LLP for general information purposes only. The presentation and related materials, if any, do not implicate any client, advisory, fiduciary, or professional relationship between you and CliftonLarsonAllen LLP and neither CliftonLarsonAllen LLP nor any other person or entity is, in connection with the presentation and/or materials, engaged in rendering auditing, accounting, tax, legal, medical, investment, advisory, consulting, or any other professional service or advice. Neither the presentation nor the materials, if any, should be considered a substitute for your independent investigation and your sound technical business judgment. You or your entity, if applicable, should consult with a professional advisor familiar with your particular factual situation for advice or service concerning any specific matters.

CliftonLarsonAllen LLP is not licensed to practice law, nor does it practice law. The presentation and materials, if any, are for general guidance purposes and not a substitute for compliance obligations. The presentation and/or materials may not be applicable to, or suitable for, your specific circumstances or needs, and may require consultation with counsel, consultants, or advisors if any action is to be contemplated. You should contact your CliftonLarsonAllen LLP or other professional prior to taking any action based upon the information in the presentation or materials provided. CliftonLarsonAllen LLP assumes no obligation to inform you of any changes in laws or other factors that could affect the information contained herein.

Session CPE Requirements

- You need to attend 50 minutes to receive the full 1 CPE credit.
- There will be 4 polling questions throughout the presentation. You must respond to a minimum of 3 to receive the full 1 CPE credit.

Both requirements must be met to receive CPE credit

Speakers

Kevin Villanueva
CISSP, CISA, PCI QSA
Principal - Cybersecurity

Julien Decosimo
CPA, MBA
Principal - Assurance

Learning Objectives

01

Identify how cyber criminals perceive nonprofit organizations as attractive targets

02

Identify the tactics used by cyber criminals to enhance their attacks and attempts at stealing information

03

Recall how AI is being used as tool for both attacking and defending networks and systems

Agenda

- Recent cyberattacks on non-profit entities
- Who are the attackers?
- Nonprofits as ideal targets
- Tactics used by cybercriminals and defenses
- Summary

Polling Question

How optimistic are you on the current economic conditions and the impact to your organization?

- 5 = Very confident
- 4 = Confident
- 3 = Neutral
- 2 = Somewhat confident
- 1 = Not at all confident

Recent Cyber Breaches on NFP Organizations

- **UNICEF (April 2024)**: “significant data breach” involving data from 11 countries by threat actor 888.
- **Save the Children International (September 2023)**: ransomware gang BianLian stole 6.8TB of data.
- **Doctors Without Borders (January 2022)**: server located in Spain was compromised. Access brokers then were selling access to the server on the Dark Web.
- **International Committee of the Red Cross (ICRC) (January 2022)**: sophisticated cyberattack resulting in data breach involving the personal information of 515,000 vulnerable people. Hampered their ability to reconnect families following disastrous events.

Who Are the Attackers?

Cybercriminal, bad actors, threat actors, attackers – all the same!

- *Nation states* – aka APTs. Well funded and resourced, motivated by financial gain, geopolitical causes, economic disruption, espionage.
- *Organized crime and ransomware gangs* – target businesses or individuals; motivated purely by financial gain.
- *Hacktivists* – ideology and social causes motivates this group. The hacktivist group Anonymous is the most famous example.
- *Insider threat actors* – employees who misuse their access to compromise data security either out of curiosity, ignorance, revenge, or financial gain.
- *Hacker* – curiosity-seeking and skilled individual looking to increase their visibility and street cred on the Dark Web.

What Makes Nonprofit Organizations Attractive Targets for Cybercriminals?

- Target rich environment!
- Operate on limited budgets with most funds dedicated to fulfilling their mission
- Perception of lack of robustness with cybersecurity controls
- Difficulty attracting cybersecurity talent
- Impact of COVID pandemic = large attack surface
- Can’t afford to divert resources following an attack

Polling Question

Which of the following is a type of bad actor/attacker?

- Hacktivists
- Malicious insiders
- Ransomware
- A and B only

Tactics Used Today

The Cyber Threat AI Poses

AI model manipulation

AI-enhanced cybersecurity attacks

AI deepfakes

Enhanced Cybersecurity Attacks

More efficient malware development and dissemination

AI-enhanced spearphishing attacks

Coming soon – autonomous agentic AI-based cyberattacks (adaptive hacking)

ChatGPT for Bad Guys

- No guardrails on responses
- Used for malware, phishing, fake content creation, deepfake creation
- Subscription based (except EvilGPT)
- Marketed on the DarkWeb

WormGPT

FraudGPT

GhostGPT

ChaosGPT

FreedomGPT

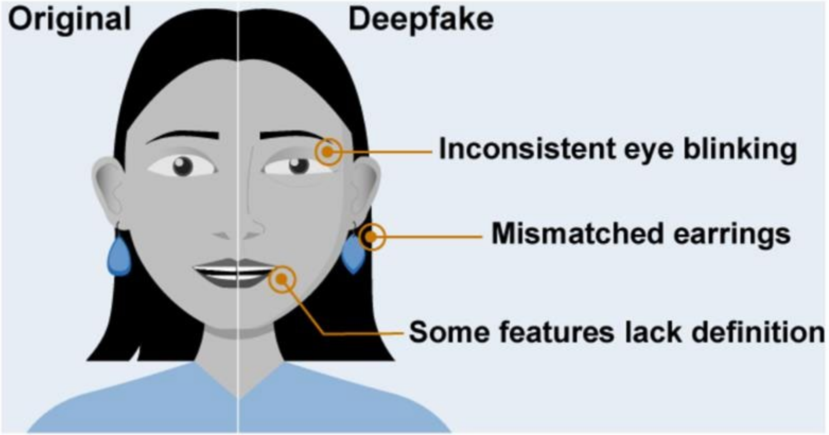
EvilGPT

Deepfakes

- “Deep learning + fake” = deepfake
- An image, or a video or audio recording that has been edited using an algorithm to replace the person in the original with someone/something else in a way that makes it look/sound authentic
- A lot of effort to make a very good, high-quality, and realistic video

AI: DeepFake Images, Videos, and Audio

- **Image Tools**: DALL-E 3, MidJourney, Adobe Firefly
- **Video Tools**: SORA, DeepSwap AI, DeepBrain AI
- **Audio Tools**: Resemble AI, iSpeech, Murf.ai



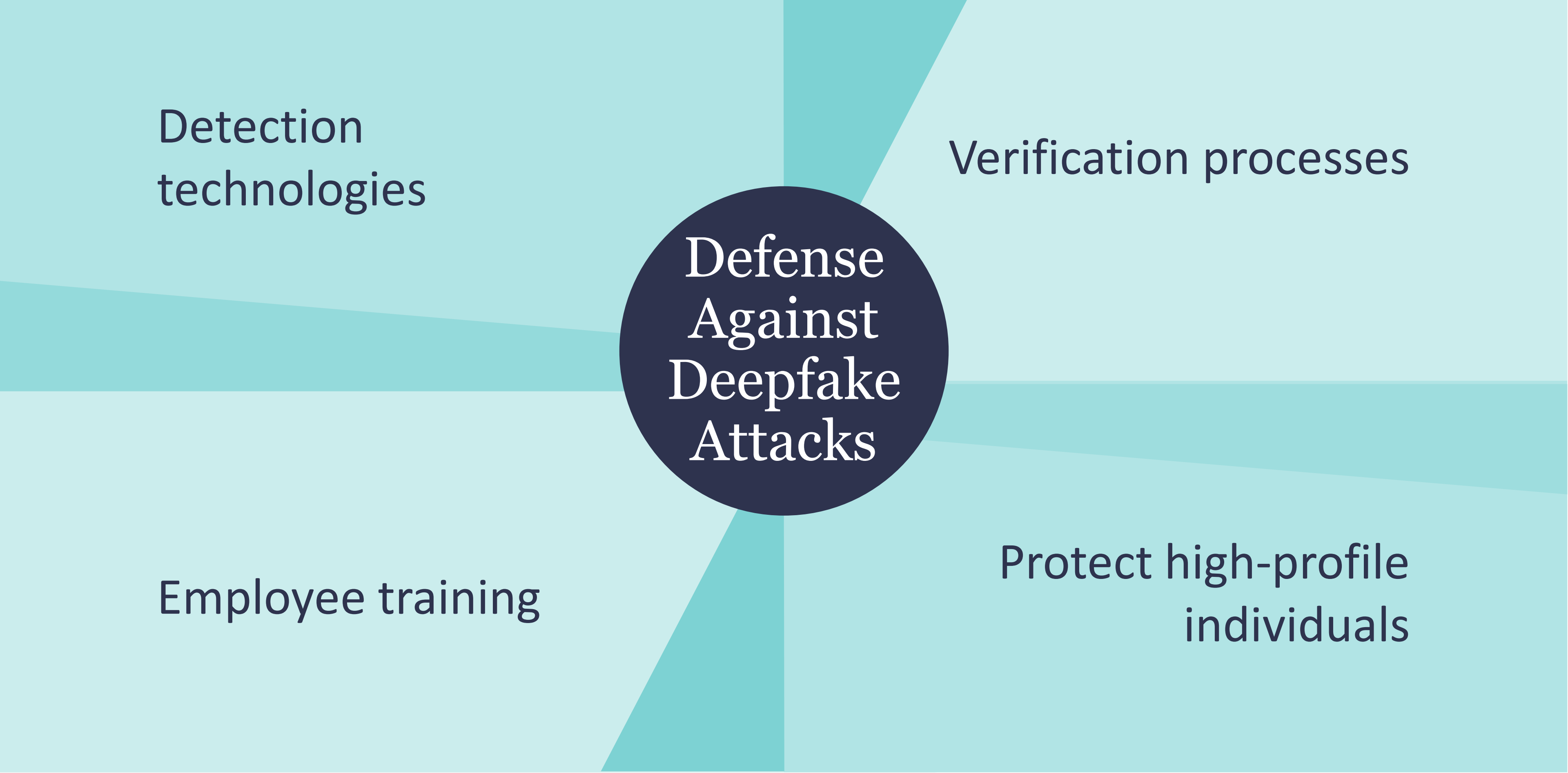
Source: GAO; conceived from DARPA image at https://www.darpa.mil/news-events/2019-09-03a. | GAO-20-379SP

AI Deepfake Impersonation

- "Finance worker pays out $25 million after video call with deepfake 'chief financial officer'" – CNN
  - Fraudster invited employee to a video call where several deep faked "employees" were on, including the CFO.

A CLA Client Story

- Occurred in 2024
- International nonprofit
- CFO received a call seemingly from the CEO via a commonly used video messaging app
- Video was seemingly of the CEO, his likeness, and voice impersonation (tone, nuances, rate)
- Request was to transfer $10 million
- Board approved the transfer and CFO executes it
- Found out later it was a fraudulent transaction involving deep fake AI technology



Defense Against Deepfake Attacks

Detection technologies

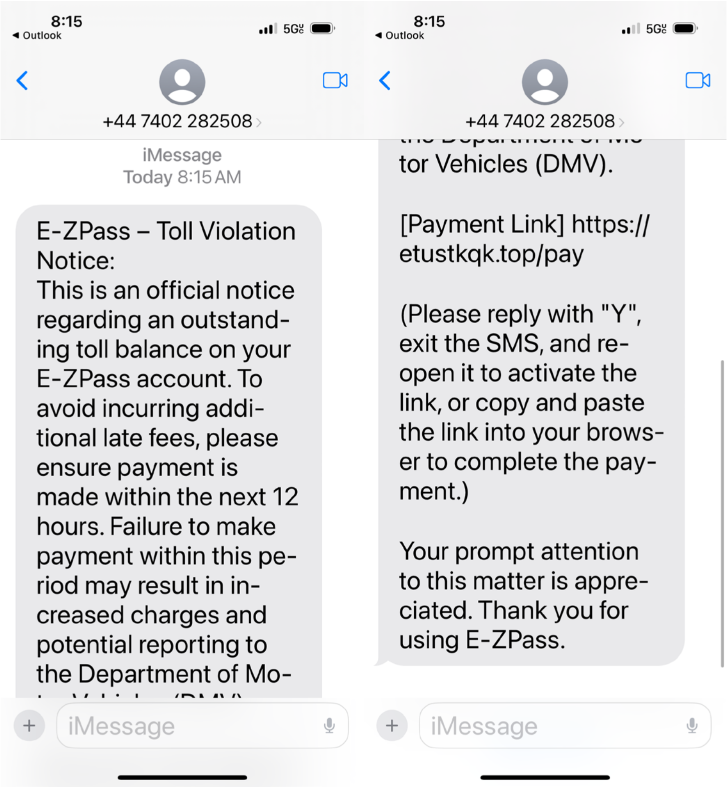
Verification processes

Employee training

Protect high-profile individuals

Smishing Attacks

- Seemingly comes from a plausible source
- Conveys urgency and consequence
- Includes a URL link to a payment site
- Sometimes more personalized



+44 7402 282508

iMessage
Today 8:15 AM

E-ZPass – Toll Violation Notice:
This is an official notice regarding an outstanding toll balance on your E-ZPass account. To avoid incurring additional late fees, please ensure payment is made within the next 12 hours. Failure to make payment within this period may result in increased charges and potential reporting to the Department of Motor Vehicles (DMV).

[Payment Link] https://etustkqk.top/pay

(Please reply with "Y", exit the SMS, and reopen it to activate the link, or copy and paste the link into your browser to complete the payment.)

Your prompt attention to this matter is appreciated. Thank you for using E-ZPass.

Defense Against Smishing Attacks

- Take note of the phone number
- Determine applicability to you
- Determine if the URL link makes sense
- Never click on the payment link
- Ignore text and wait
- Employee security awareness training
- Mobile device management (MDM) solutions

Quishing Attacks

- Another means of social engineering
- Divert the user to fraudulent or malicious websites
- Can bypass traditional phishing defenses since sent as an image
- Difficult to distinguish between legitimate and malicious QR codes

Defense Against Quishing

Verify URLs: always check the URL associated with a QR code before entering any personal information

Be cautious: avoid scanning QR codes from unknown or untrusted sources

Use security software: detects and blocks malicious websites. (e.g., Norton, McAfee, and BitDefender Mobile Security)

Fake Employee (North Korean IT Workers)

1 Nation state-sponsored Advanced Persistent Threat (APT)

2 Normal job seeking channels used (e.g., LinkedIn, Indeed, etc.)

3 Targeted WFH/remote work positions (e.g., software development) with fake resumes

4 Team in US setup laptop farms to remotely connect

5 Paychecks went to North Korean government

6 At the same time, data theft attempted

Polling Question

Would you like a CLA professional to contact you to discuss improving your cybersecurity posture and minimizing the risk of falling victim to ever evolving cyber threats and attacks?

- Yes, we could use guidance now.
- Yes, perhaps later this year.
- Not at this time.

Conclusion

Threats continue to evolve, especially given advancements in technology (i.e., AI)

Nonprofits should realize they’re an attractive target

Leadership should do their part to instill a culture of cybersecurity in the organization

Follow the widely available guidance and resources around recommended practices

Stay vigilant!

Thank you!

Kevin Villanueva
Principal – Cybersecurity
kevin.Villanueva@CLAconnect.com
(509) 823-2907

Julien Decosimo
Principal – Assurance
julien.decosimo@CLAconnect.com
(703) 825-2105

CLAconnect.com

CPAs | CONSULTANTS | WEALTH ADVISORS