

# Social Engineering Hybrid Attacks and Novel Techniques

Hacking Humans Using Subterfuge & Technological  
Trickery



# About Your Presenter – Lin Clark

- 🌱 Significant experience in physical & information security working at the Federal, State, County, and Municipal levels, for OGAs, allied governments, NGOs, and across a variety of high-risk sectors in the US and abroad.
- 🌱 Current serving Director of Cybersecurity & Cybersecurity Technology.
- 🌱 Undergraduate Degrees & Diplomas in Law Enforcement & Cybersecurity.
- 🌱 International MBA focused on Intelligence & Counter-Economic Espionage.
- 🌱 Masters of Science in Global Security focused on US Homeland Security.
- 🌱 PhD Candidate in Cybersecurity focused on the Criminal Use of Technology.
- 🌱 Contract Subject Matter Expert (SME), Keynote Speaker & Educator.
- 🌱 Professional Con-Artist & Honest Liar (Honestly).





## Defining What “Social Engineering” Is, and What it Isn’t + a Live Demo



# Defining What “Social Engineering” Is, and What it Isn’t

## **Social Engineering isn’t a new phenomena:**

- Consider the Oracle at Delphi.

## **Today, it’s thought of as a subset of Cybersecurity because of how it’s applied.**

## **At its core, it’s the exploitation of people by leveraging inescapable truths:**

- Human beings are way “stupider” than we like to admit (I’m a perfect example);
- We can easily be manipulated, influenced, persuaded, and ultimately conned;
- Humans always have access to the assets that are being protected by security technology; and
- Human beings are way “stupider” than we like to admit (did I mention, I’m a perfect example?).

## **It works because “social engineers” target our humanity and take advantage of:**

- Our social programming (such as, to be polite and trust authority in a vest with a clipboard);
- Our assumptions that messages or the voice we hear are from people we can trust; and
- A ton of cognitive biases, expectations, beliefs, and multisensory illusions.



# The Human Lie Detector – Live Demo

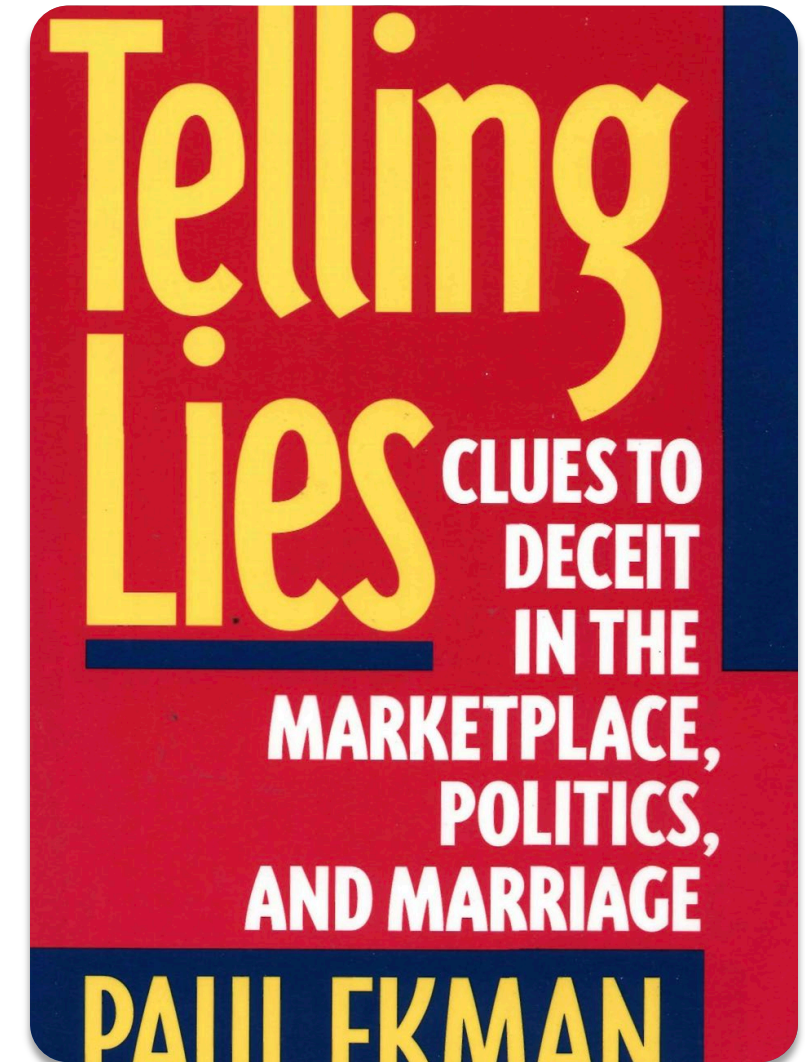
## 🌱 Dr. Paul Ekman is considered the father of understanding

### Facial :

- He is Professor of Psychology at the University of California San Francisco and a world-renowned expert in emotions research and nonverbal communication;
- He is a pioneer in the field and has spent more than 50 years studying the topic;
- He's the author of significant scientific studies and published academic works such as "Unmasking the Face", "Telling Lies", and the "Facial Action Coding System";
- His work is used by major governmental agencies such as the Secret Service; and
- I'm a student of his work, taken his courses, and I'm an instructor on allied topics.

## 🌱 In this totally unrehearsed demonstration you will see:

- One of your colleagues is a skilled liar (and why you should never trust them again);



# LIVE DEMO

## The Human Lie Detector

# SPOILER ALERT

I Exploited Cognitive Bias



## What Are “Hybrid Attacks” And Why Do They Even Matter?





# What Are “Hybrid Attacks” And Why Do They Even Matter?

## What is a so-called “Hybrid Attack” from a Cybersecurity perspective?

- It's the use of social engineering skills to facilitate technological (ie, gain access to a database) attacks;
- The use of a technology (ie, email or voice fakes) to enable a social engineering attacks (ie, to gain access to a database); and
- It always includes an effort to manipulative human behaviour to achieve the desired outcome.

## What's unique about “Hybrid Attacks”

- It can be used to overcome technology by getting someone to act on an attacker's behalf; and
- It can overcome an attacker's limits by imitating a website or access control, or even mimicking a voice;

## It should matter to every one of you because:

- Every day individuals send gift cards worth thousands of dollars to their “boss” via text message;
- Every day employees click on emails from their “IT Department” to “update their password” immediately;
- Every day people trust the voice they know on the other end of a call, and do what they're asked to do;
- Humans (read, you) are the weakest link.
- Look to the Left; Look to the right; if you're not in on the scam, you're the target.



# Exploitation at the Intersection Where Technology and Humanity Converge



# Exploitation at the Intersection Where Technology and Humanity Converge


- 🌱 **As technology safeguards increase, hybrid attacks grow:**
  - From the user's perspective, little has changed.
- 🌱 **If only there were a way to trick someone:**
  - Enter thousands of advanced, specialized, free programs available to anyone.
- 🌱 **An example is the WiFi Password Stealer Fluxion**
  - Very well written and contains many router branded templates.
  - Fully automated with a menu driven interface.
  - Mimics the target's WiFi.
  - Directs user by blocking access to their WiFi.
  - Once they join tells them: "You have been blocked by your ISP - Please prove you're the owner of this router by providing the WPA key".
  - Checks the password against a WPA Handshake.
  - Stops blocking access once correct password was provided.
  - Fluxion hacks the user, not the technology. It's the path of least



```
Site: https://github.com/FluxionNetwork/fluxion  
FLUXION 6 (rev. 9) by FluxionNetwork  
Online Version [6.9]  
  
[*] aircrack-ng..... OK.  
[*] bc..... Missing!  
[*] awk..... OK.  
[*] curl..... OK.  
[*] cowpatty..... Missing!  
[*] dhcpcd..... Missing!  
[*] 7zr..... OK.  
[*] hostapd..... Missing!  
[*] lighttpd..... Missing!  
[*] iwconfig..... OK.  
[*] macchanger..... OK.  
[*] mdk4..... Missing!
```

# Exploitation at the Intersection Where Technology and Humanity Converge

- 🌱 **Big deal, WPA is nothing. What about more sophisticated security?**
  - No worries, hackers move in real time and are dynamic.
- 🌱 **An example of MITM credential and 2FA token theft program**
  - Acts as both Web Server and DNS Server in one.
  - Modular framework for extensibility and compatibility with many services.
  - Workflow is straight forward:
    - Purchase a look-alike domain in non-extraditable country;
    - Spin up VPS allowing 80, 443, 53(UDP) inbound;
    - Point NS records to VPS;
    - Configure server and “phishlets” you want to target;
    - Build a sophisticated phishing email;
    - Send it and wait for a bite;
    - Add new device to victims 2FA enrolment portal.

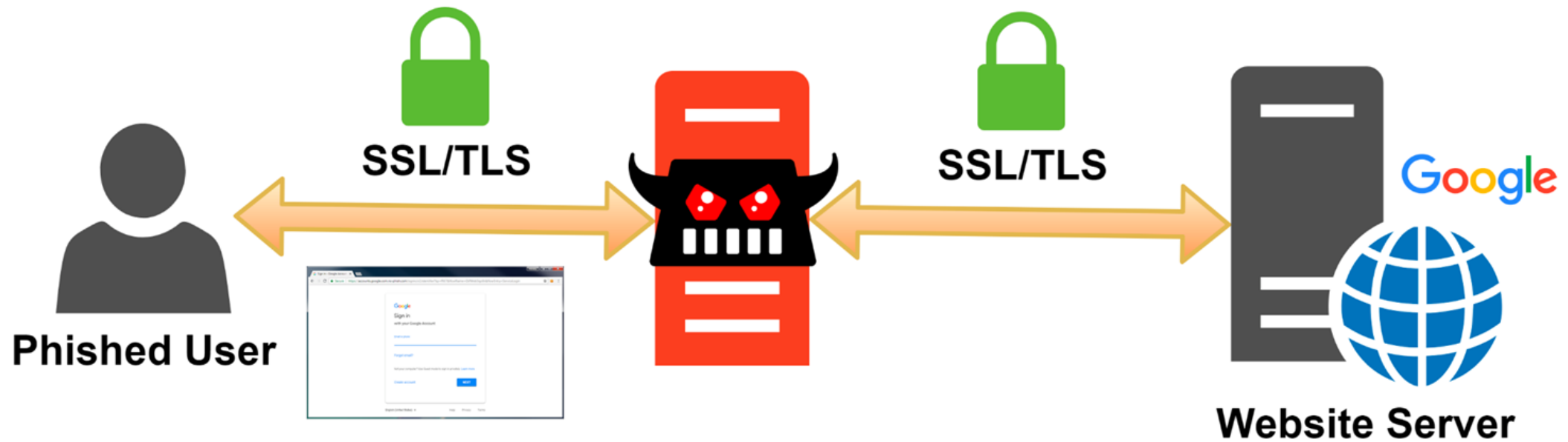


The screenshot shows the Evilginx terminal interface. At the top, there's a red header with a pixelated character and the text "Evilginx" in a stylized font. Below the header, it says "-- Gone Phishing --" and "by Kuba Gretzky (@mrgretzky) version 2.4.2". The main part of the terminal displays configuration logs for loading phishlets, configuration files, blacklist mode, redirect parameters, verification parameters, and tokens. It also shows a warning about a failed nameserver start and server configuration details for domain and IP.

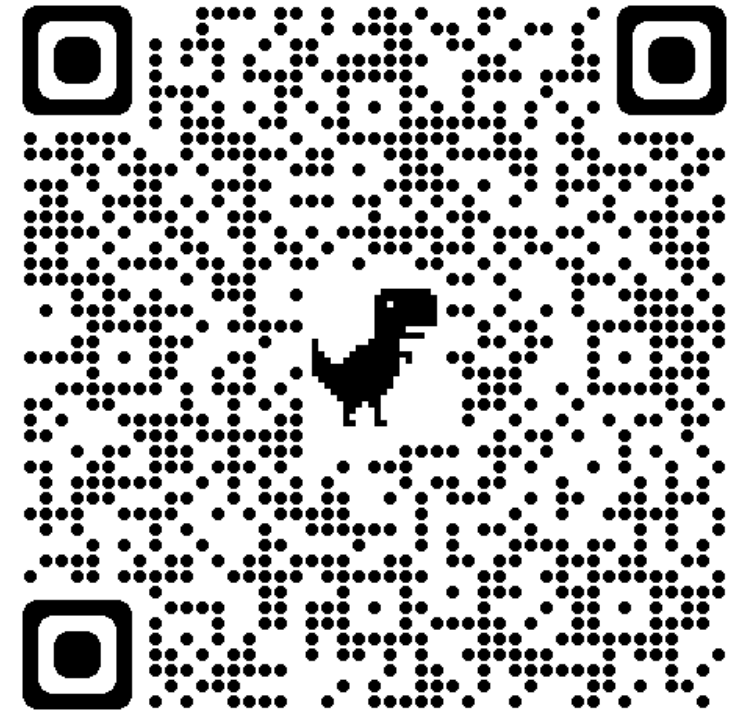
phishlet	author	active	status	hostname
book	@charlesbel	disabled	available	
agram	@charlesbel	disabled	available	
ook	@mrgretzky	disabled	available	
it	@customsync	disabled	available	
press.org	@meitar	disabled	available	
on	@customsync	disabled	available	
ix	@424f424f	disabled	available	
base	@An0nUD4y	disabled	available	
ok	@An0nUD4Y	disabled	available	
	@jamescullum	disabled	available	
ogin	@perfectlylog...	disabled	available	
onmail	@jamescullum	disabled	available	
ter-mobile	@white_fi	disabled	available	
al	@An0nUD4y	disabled	available	
ter	@white_fi	disabled	available	
nb	@An0NUD4Y	disabled	available	
ing	@Anonymous	disabled	available	
ub	@audibleblink	disabled	available	
edin	@mrgretzky	disabled	available	
	@mikesiegel	disabled	available	



## Example of Hybrid Attack Set-Up Using Free Software



## US Department of Homeland Security & FBI Report On Increasing Risk of DeepFake Technology



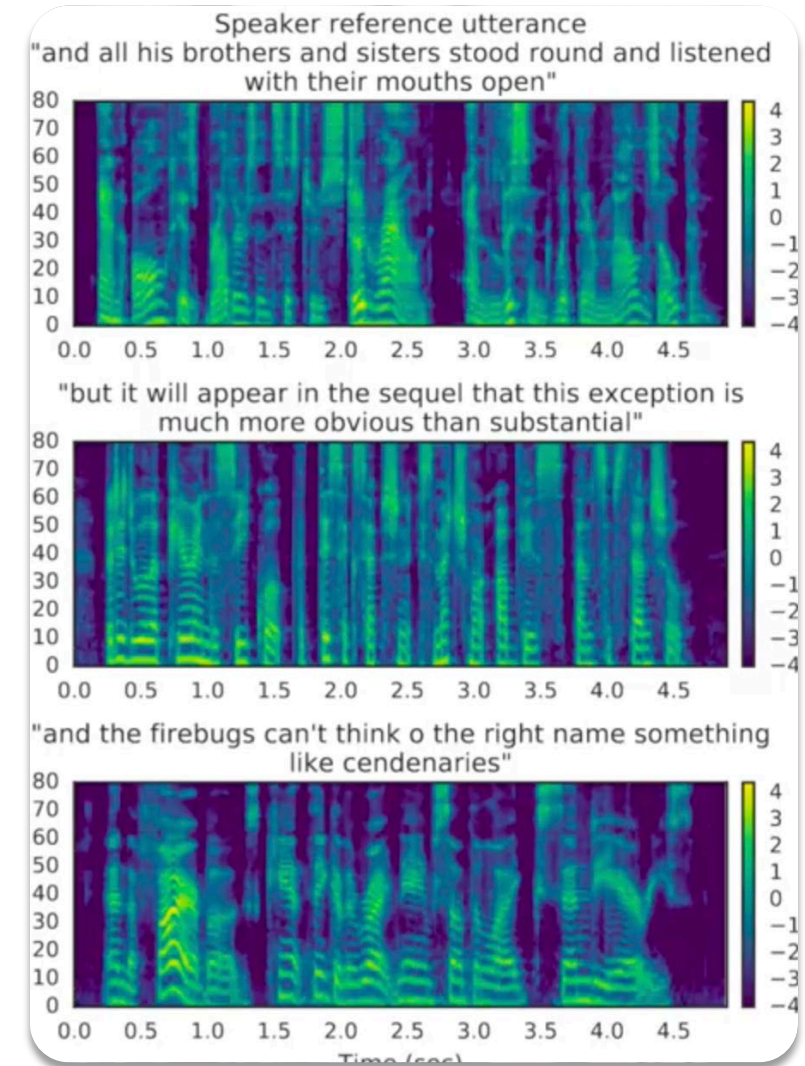
# Exploitation at the Intersection Where Technology and Humanity Converge

## 🌱 DeepFakes are becoming an increasing threat to everyone:

- Falls under the greater and more pervasive umbrella of synthetic media;
- Uses artificial intelligence/machine learning (AI/ML) to create believable, realistic videos, pictures, audio, and text of events which never happened

## 🌱 A notable example of Audio DeepFake used to attack the human:

- A bank manager in Hong Kong was contacted by the "Director" of the company with instructions to wire money;
- The bank manager recognized the "voice" of the "Director", who he met before, and acted on his orders;
- Unbeknownst to the bank manager, fraudsters used "deep voice" technology to clone the director's speech;
- The bank manager wired over \$30 million dollars to the criminals;
- The money was wired to numerous numbered bank accounts all over the world;
- What was once science fiction, is now reality and widely available.




## CYBER-CRIME

### FBI warning: Crooks are using deepfake videos in interviews for remote gigs

23 

Yes. Of course I human. Why asking? Also, when you give passwords to database?

 [Laura Dobberstein](#)

Wed 29 Jun 2022 // 06:16 UTC




The US FBI issued a warning on Tuesday that it has received increasing numbers of complaints relating to the use of deepfake videos during interviews for tech jobs that involve access to sensitive systems and information.

The deepfake videos include a video image or recording convincingly manipulated to misrepresent someone as the "applicant" for jobs that can be




# Exploitation at the Intersection Where Technology and Humanity Converge



## Public Service Announcement

FEDERAL BUREAU OF INVESTIGATION



**June 28, 2022**

**Alert Number**  
**I-062822-PSA**

Questions regarding this  
PSA should be directed to  
your local **FBI Field Office**.

Local Field Office Locations:  
[www.fbi.gov/contact-us/field-offices](https://www.fbi.gov/contact-us/field-offices)

### Deepfakes and Stolen PII Utilized to Apply for Remote Work Positions

The FBI Internet Crime Complaint Center (IC3) warns of an increase in complaints reporting the use of deepfakes and stolen Personally Identifiable Information (PII) to apply for a variety of remote work and work-at-home positions. Deepfakes include a video, an image, or recording convincingly altered and manipulated to misrepresent someone as doing or saying something that was not actually done or said.

The remote work or work-from-home positions identified in these reports include information technology and computer programming, database, and software related job functions. Notably, some reported positions include access to customer PII, financial data, corporate IT databases and/or proprietary information.

Complaints report the use of voice spoofing, or potentially voice deepfakes, during online interviews of the potential applicants. In these interviews, the

Source: <https://www.ic3.gov/Media/Y2022/PSA220628>

# Exploitation at the Intersection Where Technology and Humanity Converge

CRYPTOCURRENCIES

## Hackers Use Deepfakes of Binance Exec to Scam Multiple Crypto Projects

The crypto exchange's CCO Patrick Hillman wrote that he received multiple messages thanking him for meetings he never attended.

By Kyle Barr | 8/23/22 2:35PM | Comments (7) | Alerts



Binance is often rated as the top crypto exchange by trading volume, and so it's become a high value target for scammers who pretend to be exchange execs in meetings with various crypto projects.

Photo: Ilyna Budanova (Shutterstock)

A recent report from a Binance executive reads more like a tech lingo bingo card than a warning about online stranger danger. Apparently going the usual route to hack crypto projects was a little too "lo-fi" for some crafty scammers, as the crypto exchange announced that hackers had a hologram deepfake to defraud several crypto projects out of their funds.

[Binance](#) Chief Communications Officer Patrick Hillmann wrote in a [blog post](#) last week that internet scammers had been using deepfake technology to copy his image during video meetings. He started to



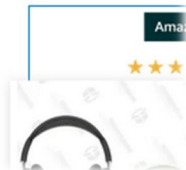
Luke Macfarlane | First F

Jacob Anderson & Sam Reid | First Fandoms

Yesterday 12:30PM

Bobby Moynihan's Favorite Moment from SNL

Wednesday 8:15AM



NEWS

## Binance chief says a "sophisticated hacking team" turned him into a deepfake hologram

CYBER-CRIME

## Here's how crooks will use deepfakes to scam your biz

11 

Need some tools of deception? GitHub's got 'em

 [Jessica Lyons Hardcastle](#)

Wed 28 Sep 2022 // 07:24 UTC



All of the materials and tools needed to make deepfake videos – from source code to publicly available images and account authentication bypass services – are readily available and up for sale on the public internet and underground forums.





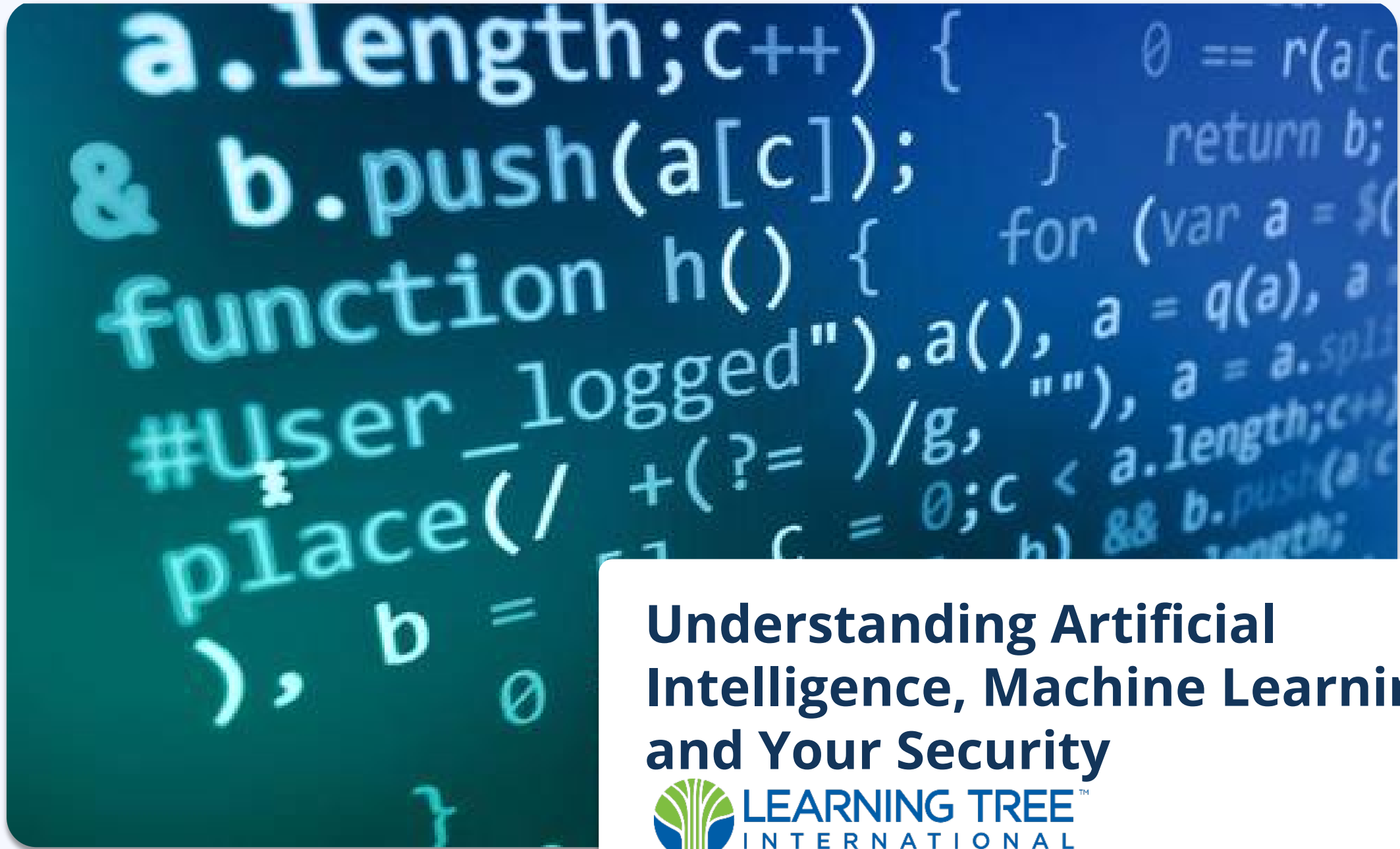
12-26-22

## Deepfakes: Get ready for phishing 2.0

With deepfakes, phishing is evolving once again and being called the most dangerous form of cybercrime.







**Understanding Artificial  
Intelligence, Machine Learning,  
and Your Security**



# Understanding Artificial Intelligence, Machine Learning, and Your Security

## What is Artificial Intelligence and Machine Learning (AI/ML)?

- It's a program that predicts result based on incoming data;
- Models for those predictions are created by ingesting (training on) data;
- It's not alive; it's code that does what we tell it to do.

## What are some examples of AI/ML?

- OpenAI
- ChatGPT
- Dall-E

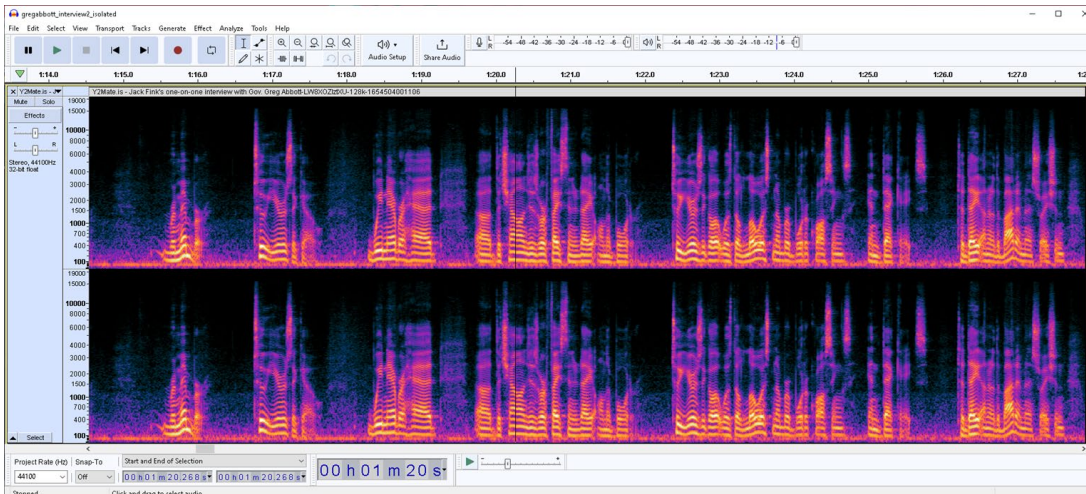
## What can we do with AI/ML?

- The use cases are fairly endless, but right now we use it to code, write, communicate, and create imagery;
- We can use ML to learn what someone's voice or face looks or sounds like;
- We can then train that model to understand how one voice or face relates to another;
- Once the model is built, it can be used to leverage your trust by impersonating someone.

# Understanding Artificial Intelligence, Machine Learning, and Your Security

## How do you impersonate someone using AI/ML?

- First, you need the right data;
- An example, may be a 5-10 second audio clip (voice) of the intended impersonation target;
- The data can be extracted from virtually any online media, recorded in real time, or taken covertly;
- Then, train the model on the data; and
- Design and execute your attack.



# LIVE DEMO

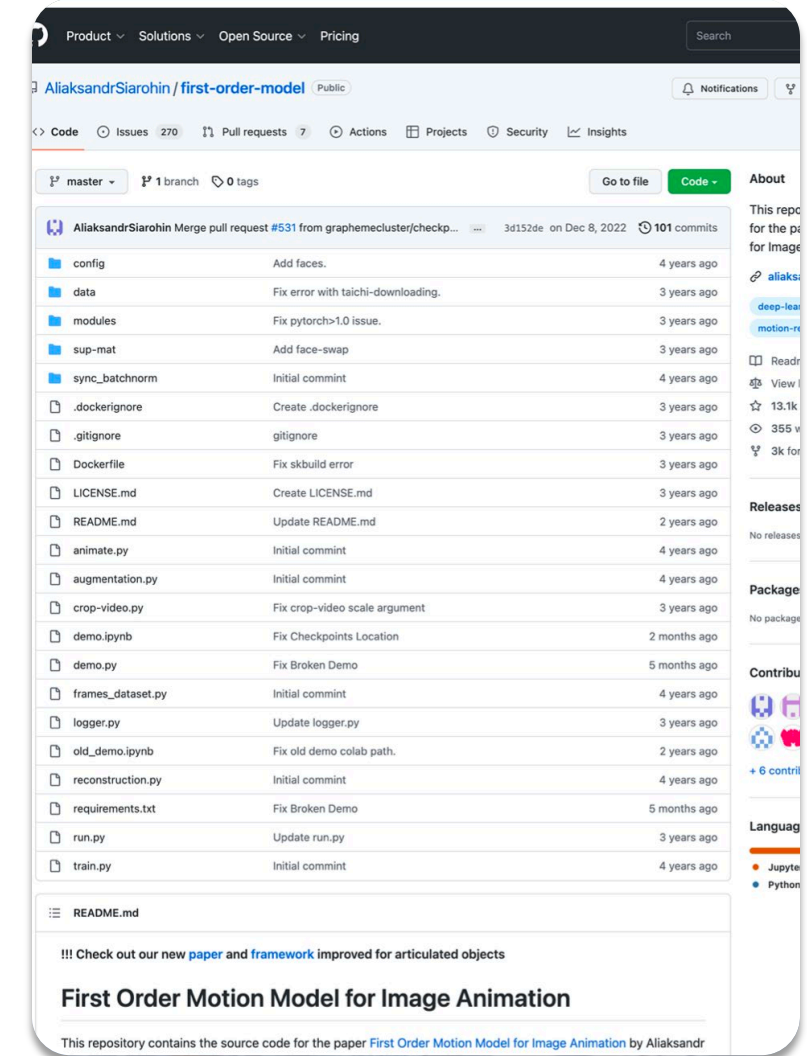
## Cloning a Known Voice



# Understanding Artificial Intelligence, Machine Learning, and Your Security

## Machine Learning tools for Video are similar to that of Voice:

- The machine learning model needs data, like a face;
- This differs from voice ML in that the data is much harder to normalise;
- To match one face to another we need two similarly positioned faces;
- The lighting and environmental must also be similar.

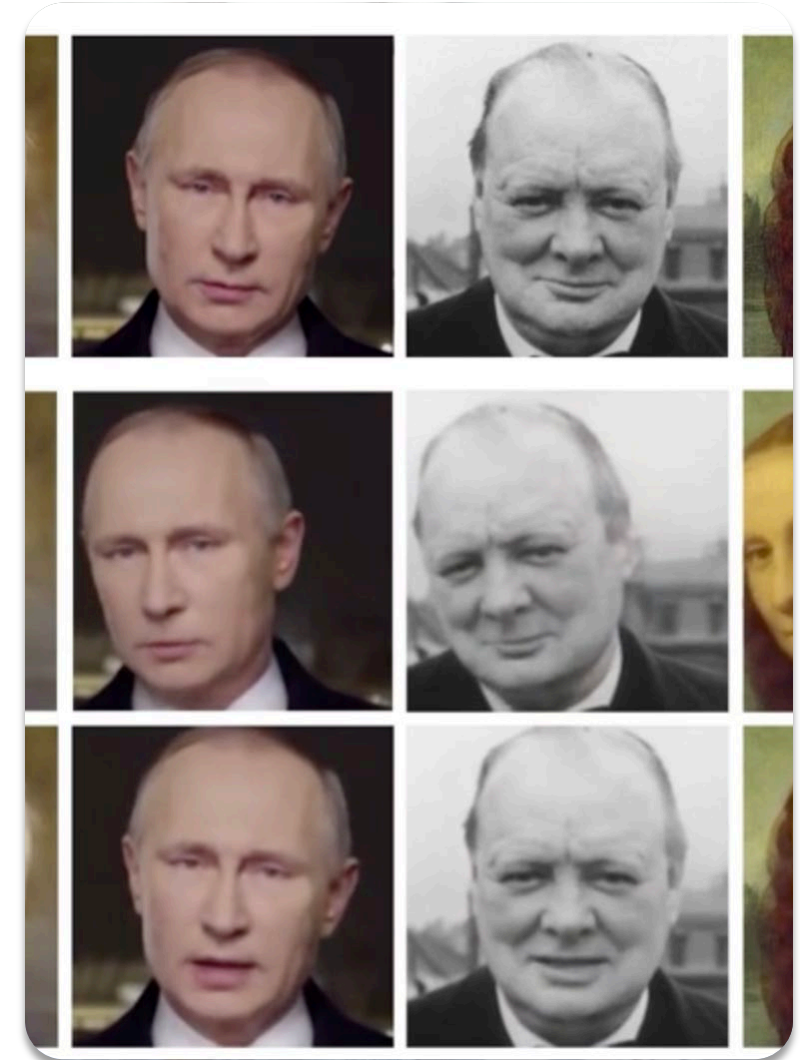


# Understanding Artificial Intelligence, Machine Learning, and Your Security

## 🌱 AI/ML isn't the only way to clone a face:

- Modern smart phones and tablets are now powerful enough to conduct real time face detection;
- Smartphones can map a 3D mesh to any face it sees in a camera;
- Apps like SnapChat Lens Studio can adjust eye and hair colour on the fly;
- Other apps change features on the fly;
- Filters in products like Zoom, Teams, and other video chat systems currently have filters that map to the face in real time.

## 🌱 It's just a matter of time before the technology can be used in real time on calls and video chats, allowing for criminals to impersonate anyone they want to. Stay tuned.





## What Steps Can I Take to Safeguard Against These Kinds of Attacks?





# What Steps Can I Take to Safeguard Against These Kinds of Attacks?

 **Don't ignore it. These are real threats that need to be addressed.**

 **The key to mitigating risks is to nurture cybersecurity instincts among employees:**

- Run security awareness training to ensure employees understand their responsibility and accountability;
- Conduct phishing simulations to give workers “hands-on” experience with deepfakes so they understand experientially;
- Train employees to watch out for visual cues such as distortions and inconsistencies in images and video
- In cases of video conferencing, ask the participant to wave their hands in front of their face and turn sideways;
- Ask users to stick to company cybersecurity policies and best practices;
- Ensure senior management actively participates in building the security culture because culture is always top-down;
- Always take a beat. Stop. Think. Before you act. Especially if you are feeling pressured or incentivised.
- If you are unsure, ask your cybersecurity department.

 **Call me. I'm happy to help!**