The Human Firewall

Some people call it Social Engineering.

Lets Talk Social Engineering

Social Engineering in its most basic form is getting someone to do something or say something they shouldn’t do or say.

Christopher Hadnagy

https://www.social-engineer.com/product/foundational-application-of-social-engineering/

If Social Engineering was a Cake!

- take 20g of almost unlimited attack surface
- mix that with 30 grams of an almost inexhaustible array of attack vectors
- add a dash of not enough training
- add a good dollop of manipulation
- bake in the oven with patience

That’s a cake that no employee wants to eat.

Statistics About Fraud

- The total value of alleged fraud over £100k reaching UK Courts in 2022 was £1.12bn.
- This is an increase of 151% compared to £444.7m in 2021.
- The volume of cases has however fallen by 27% from 298 in 2021 to 219 in 2022.
- 82% of fraud cases have some form of Social Engineering element.
- 47% of fraud cases use Social Engineering as a delivery mechanism.

Statistics About Attacks

- More than 80% of UK organizations experienced a successful attack in 2021/2022
- Over a 12-month period, ransomware attacks affected 73% of UK organizations
- 13% of UK organizations ended up paying the ransom
- Around 8% of people tried to open a phishing link in 2021 & 2022
- According to private research around 79% of spear phishing targets fell for the email.

Statistics – GDPR Fines

- The UK has issued €44 million worth of GDPR fines in 2022
- Luxembourg issued the biggest GDPR fine by far, which stands at €746 million and is against a US online retailer.
- Ireland issued a fine of €225 million against WhatsApp Ireland Limited.
- IBM investigated the root cause of breaches and found that 53 percent of UK breaches were malicious in nature. 22 percent were caused by system glitches and 25 percent by human error.

Some Businesses Have it Wrong!

I'm here to tell you that we need to make a change.

A big change that every forward-thinking company must make.

What's the Change?

We need to stop giving substandard Social Engineering training!

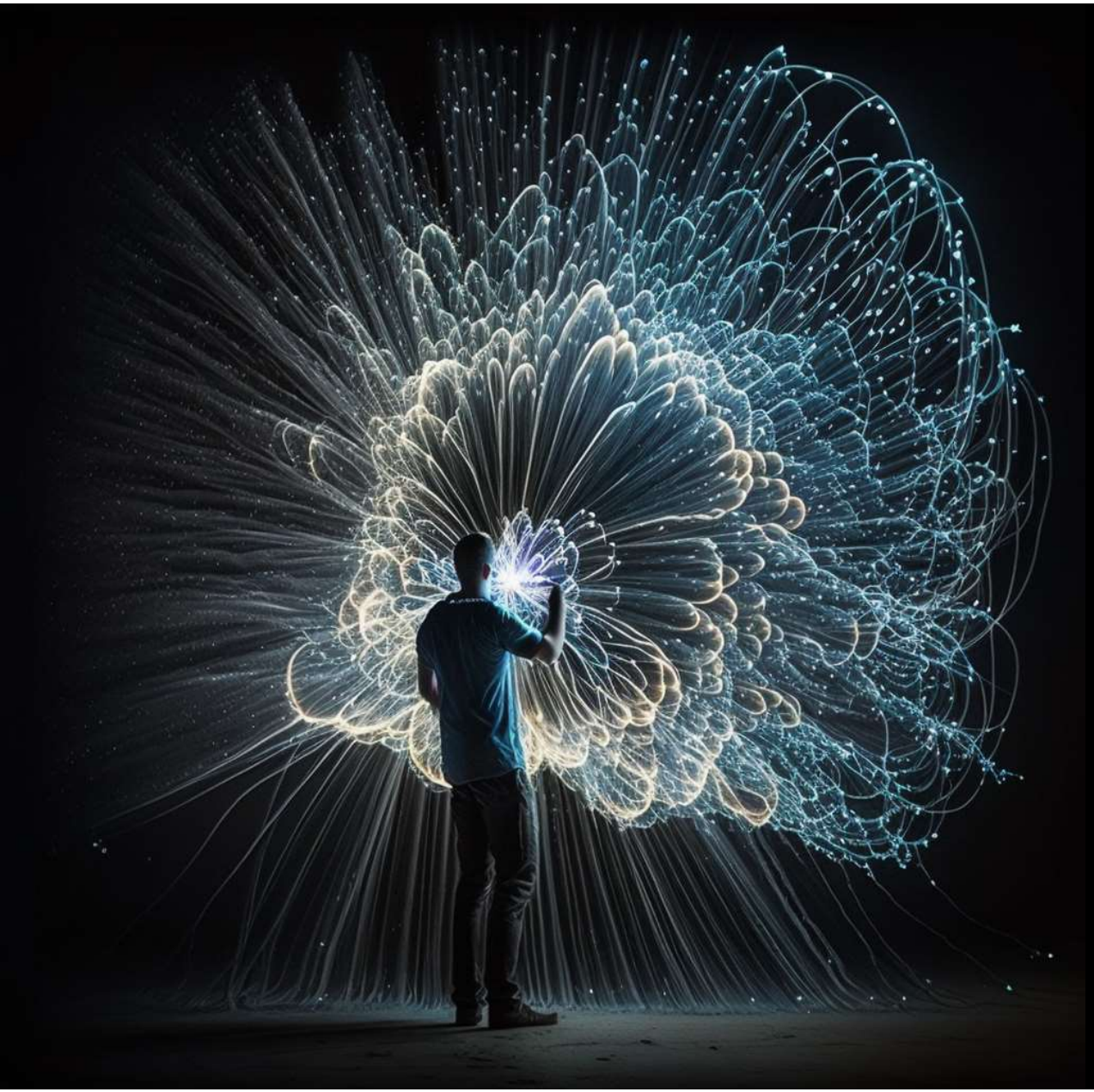
This gives both companies and its staff the illusion of being safe when in fact, it makes it even easier to attack.

I cannot stress this point enough…

Paradoxes

There are several paradoxes that exist. We will take a quick look at a some of them.

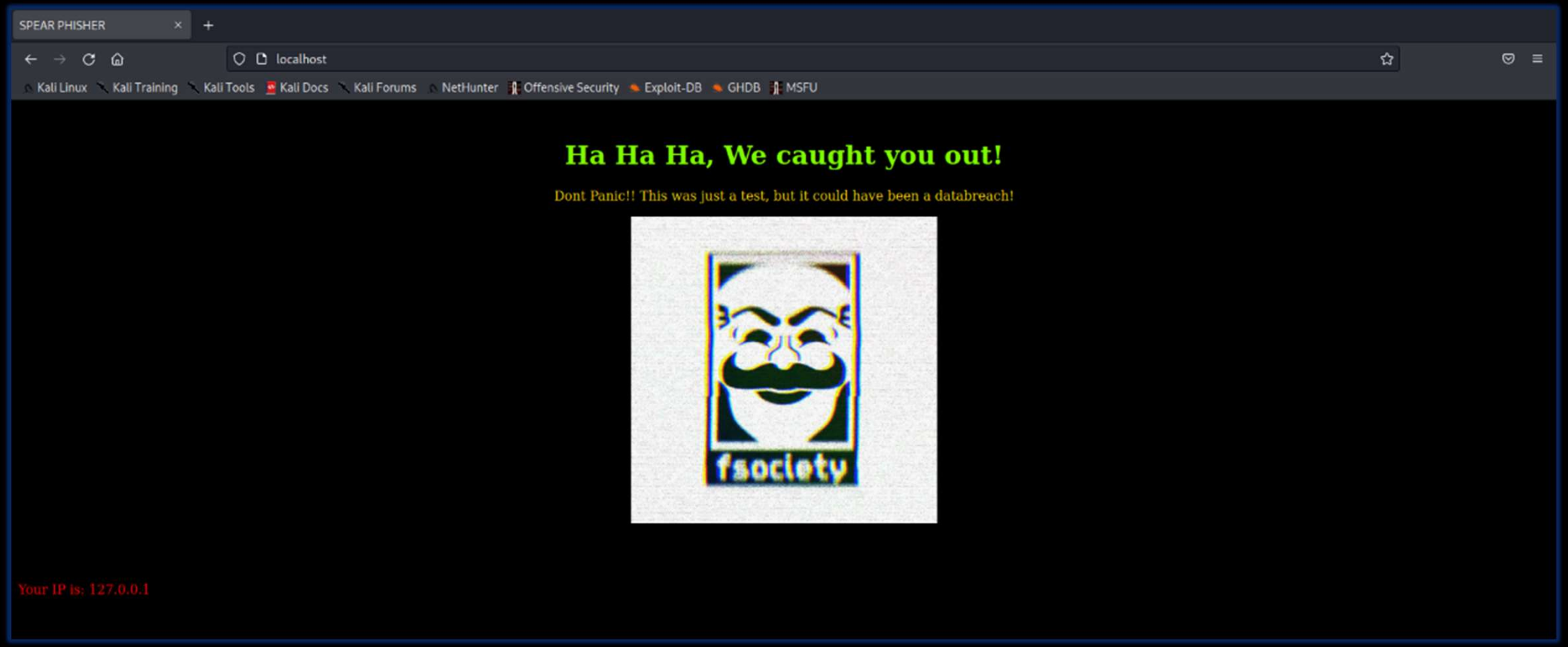
- Learning Paradox
- Antivirus Paradox
- Nessus Scanning Paradox
- Technical Mitigation Paradox
- Social Engineering Training Paradox



A Recent Test

- I recently was asked to attack a company who I am unable to name.
- We created a document of scope which took a long time
- They had 46 members of staff who all worked remotely.
- They were a very forward thinking company who took their cyber security very seriously.
- There was one person who’s responsibility was their server side technology,
- My goal was to attempt to get them to click a link.
- They were already aware of these dangers and had received training which was better than most.

Step 1 – Setup a webserver and make a page.



Step 2 – Add the following code to the visitors IP address.

Note: This could be setup to serve malware to the target.

```php
// IP Logger

// Show Warning on Screen


echo "Your IP is: ".$_SERVER['REMOTE_ADDR'];

// Get IP
$ip = $_SERVER['REMOTE_ADDR'];


// Get Gio Location usinf IP-API site
$query = @unserialize(file_get_contents('http://ip-api.com/php/'.$ip));


//Open the Log File
$handle = fopen("data.txt", "a");

// Writes IP Addr to Log File
fwrite($handle, "IP: $ip \r\n");


// Writes Date & Time to the Log File
fwrite($handle,date('Y-m-d H:i:s'));


// Writes to next line
fwrite($handle,"\n");


// If the IP-API comes back success set write parameters
if($query && $query['status'] == 'success') {
$hh = $query['country'].', '.$query['city'].'!';


// Fwrites location if successful otherwise notetifies failed attempt
fwrite($handle, "Location: $hh \r\n \r\n");
} else {
  fwrite($handle, "Location: Unavailable \r\n \r\n");
}

// Writes to next line twice
fwrite($handle,"\n");
fwrite($handle,"\n");


// closes file
fclose($handle);
```

Step 3 – Carry out extensive OSINT and write some Spear Phishing emails based upon your findings.

ROYAL AIR FORCE AIR CADETS the next generation

[redacted] **Squadron**

RE: [redacted]

We have recently been made aware that [redacted] **Squadron** is losing up to 75% of its Ministry of Defence funding at the start of the new tax year in April 2023.

Since we will only have 25% of the original funding, it may make it impossible to continue operating.

We feel that this is terrible news, as a lot of young people depend on us, therefore, we would like to invite you to sign our online petition.

Save [redacted] Squadron Online Petition at change.org

Your Sincerely

[redacted]

Flight Lieutenant RAFAC

Step 4 – Using BASH, write a super simple tool to spoof email using an online SMTP server such as SendInBlue.

```
#!/bin/bash

figlet "mail smasher" | lolcat

echo
echo

read -p "Who do we send the emails to? > " emailTO
read -p "What is the sending email? > " sender
read -p "What would you like the subject to be? > " subject
read -p "How many emails do you want to send? > " numberOfMails
read -p "What time would you like between sends in seconds? > "
emailTime
read -p "What is the HTML file containing the message body? > "
htmlFile

for i in $(seq 1 $numberOfMails);
do
  echo "Sending email #$i..."

  sendemail -xu tompdjohnson@outlook.com -xp kPIfZUYQzO1gtHK8 -s
smtp-relay.sendinblue.com:587 -f "$sender" -t "$emailTO" -u "$subject"
-o message-file="$htmlFile" -o message-content-type=html 2>/dev/null

  sleep $emailTime
done

echo "All emails sent."
```

Step 5 – Send email with your custom message to the target or targets and await them visiting your page.

Your targets ‘Click the Link’ and your weaponised Apache Webserver does its thing…

Its that easy!

But this didn’t work!

But fortunately for me, most people are easy to manipulate…

So how did I turn it around?

Making the best of a bad Situation

Hi all,

As you maybe aware we are currently under attack with a range of sophisticated phishing emails. Luckily this is part of a test, but this does not mean we should let our guard down. I have created a check list to help you secure your emails

https:/ /cybersecurity/emailchecklist.doc

Please ensure that you read and digest as much as possible. If in any doubt please contact me.

Thanks

Presidential Election

Some people are good at spotting malicious emails. In fact, both Podesta and Clinton were suspicious of the phishing emails they received. Before clicking, Podesta even asked his tech-support staff if a link was legitimate.

Those experts should have known how to spot a spear phishing attack but failed.

They told him to click on the malicious link and then America was awarded TRUMP as a prize!

If the US Government can fall for a spear phish, how likely are your staff to fall for one? EDUCATE, TRAIN, PREPARE!

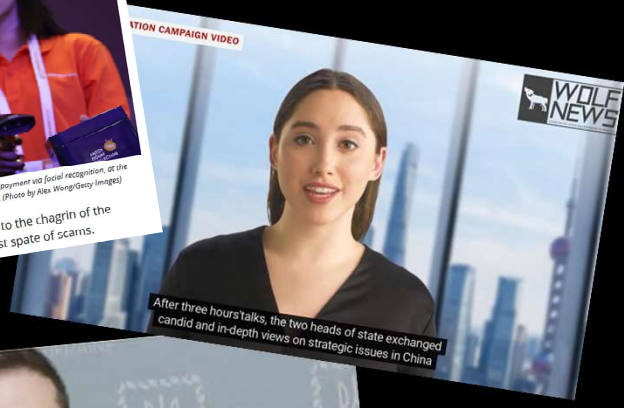
What is the Future of Social Engineering?

Deepfakes widen fraud opportunities for financial hackers

Karen Hoffman December 8, 2021

An Alibaba employee demonstrates "Smile to Pay," an automatic payment system that authorize payment via facial recognition, at the Alibaba booth during CES 2017 at the Las Vegas Convention Center on Jan. 5, 2017, in Las Vegas. (Photo by Alex Wong/Getty Images)

Cyber-thieves are learning to "fake it till they make it," much to the chagrin of the financial service institutions who are falling prey to this latest spate of scams.



This PSA About Fake News From Barack Obama Is Not What It Appears

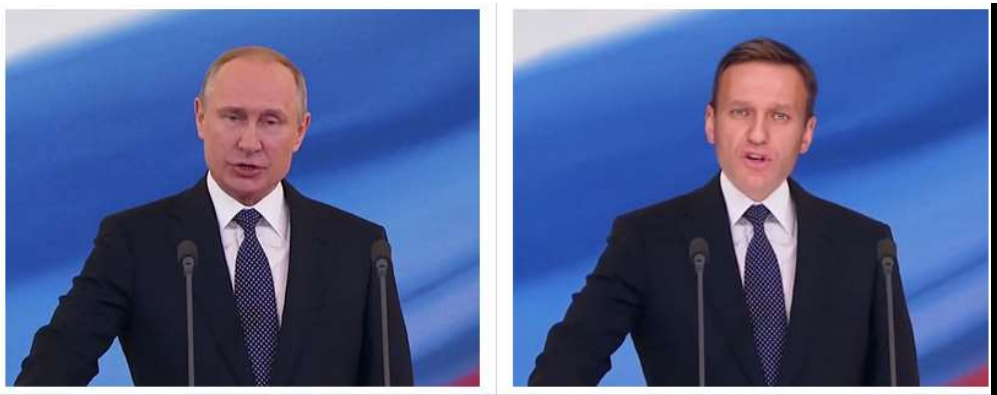
Oscar-winning filmmaker Jordan Peele has a warning for viewers about trusting material they encounter online.

David Mack
BuzzFeed News Reporter

Posted on April 17, 2018, at 11:28 a.m. ET

Tweet Share Copy

Sitting before the Stars and Stripes, another flag pinned to his lapel, former president Barack Obama appears to be delivering an important message about fake news — but something seems slightly...off.



https://www.youtube.com/watch?v=xr5FHd0AdlQ

https://www.youtube.com/watch?v=RTjgkhMugVw

What is DeepFaceLab?

DeepFaceLab is one of the leading software tools being used for creating deepfakes right now.

Its Available for free on Windows and hosted on Github, it has become extremely accessible and led to a number of tutorials on the service online

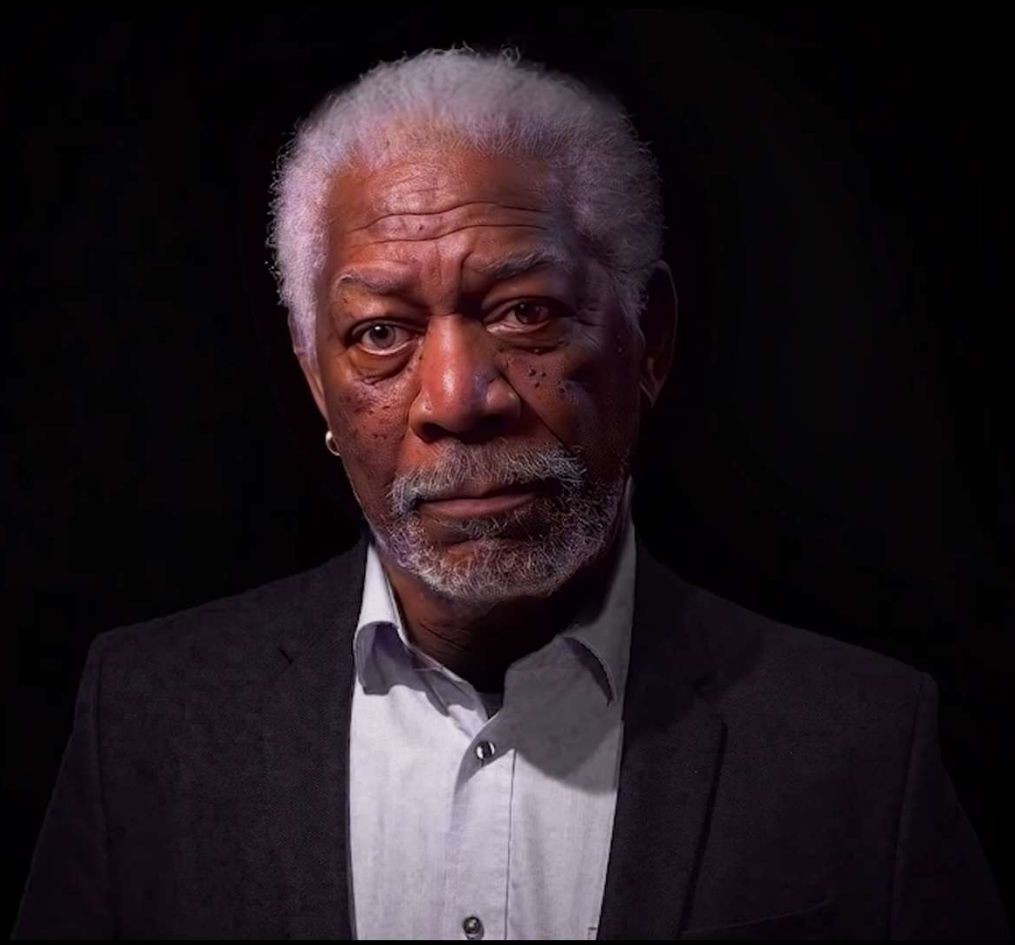
The DeepFaceLab 2.0 requires lots of processing power so its recommended you use atleast 1 NVIDIA RTX 3000 series GPU which specifically supports Tensor Core processing.

[Download it here: https://github.com/iperov/DeepFaceLab](https://github.com/iperov/DeepFaceLab)

Kim Jong Un Propaganda Video - 3 Years Old Technology

Startrek Video 2 Years Old Technology

Video 1 Year Old Technology



4 seconds?

FORBES > INNOVATION > CONSUMER TECH

A Voice Deepfake Was Used To Scam A CEO Out Of $243,000

Jesse Damiani Contributor ⓘ
I run Postreality Labs, a sensemaking & strategy studio.

Follow

Sep 3, 2019, 04:42pm EDT

This article is more than 3 years old.

Anonymous hacker programmer uses a laptop to hack the system in the dark. Creation and infection of ... [+] GETTY

It's the first noted instance of an artificial intelligence-generated voice deepfake used in a scam.

Phone scams are nothing new, but the mark usually isn't an accomplished CEO.

AI Voice Technology

According to a new report in *The Wall Street Journal*, the CEO of an unnamed UK-based energy firm believed he was on the phone with his boss, the chief executive of firm's the German parent company, when he followed the orders to immediately transfer €220,000 (approx. $243,000) to the bank account of a Hungarian supplier.

Where to get it?

Setup

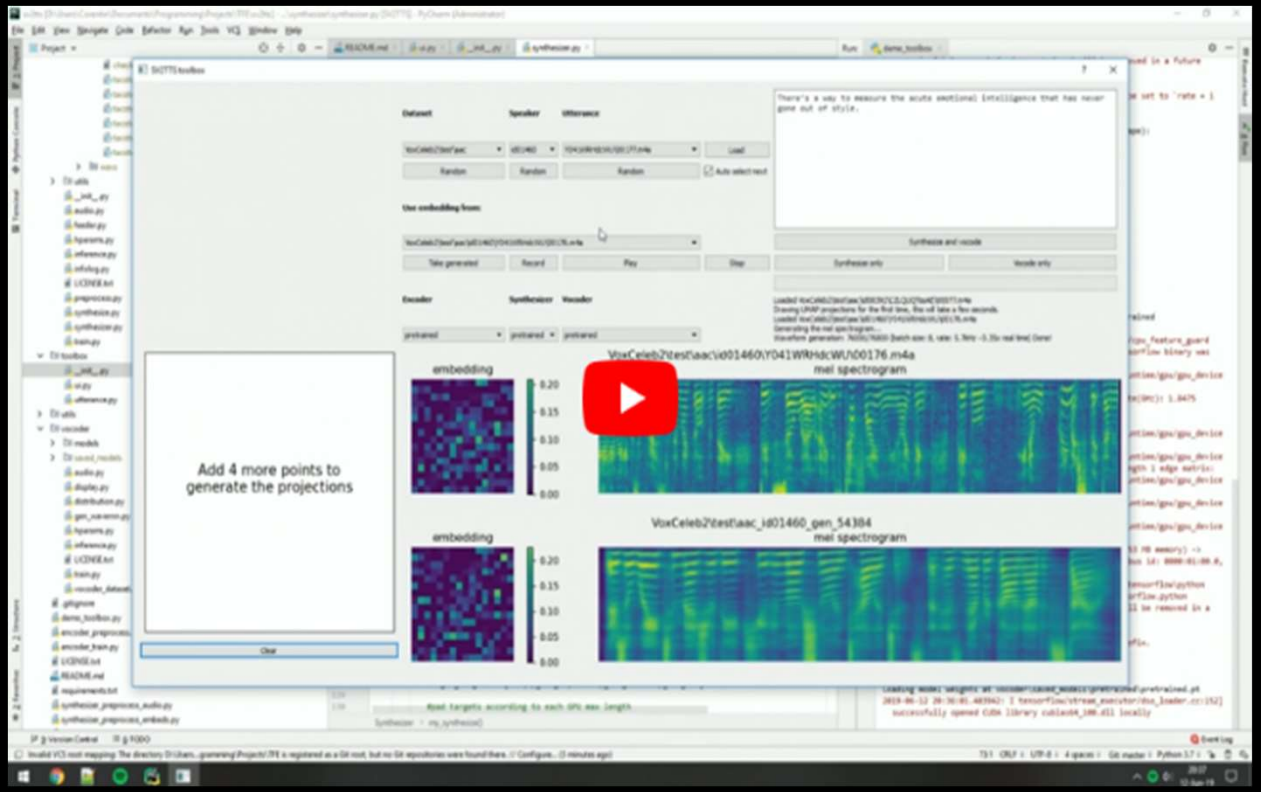
1. Install Requirements
1.Both Windows and Linux are supported. A GPU is recommended for training and for inference speed, but is not mandatory.
2.Python 3.7 is recommended. Python 3.5 or greater should work, but you'll probably have to tweak the dependencies' versions. I recommend setting up a virtual environment using venv, but this is optional.
3.Install ffmpeg. This is necessary for reading audio files.
4.Install PyTorch. Pick the latest stable version, your operating system, your package manager (pip by default) and finally pick any of the proposed CUDA versions if you have a GPU, otherwise pick CPU. Run the given command.
5.Install the remaining requirements with pip install -r requirements.txt

2. (Optional) Download Pretrained Models
Pretrained models are now downloaded automatically. If this doesn't work for you, you can manually download them here.

3. (Optional) Test Configuration
Before you download any dataset, you can begin by testing your configuration with:
python demo_cli.py
If all tests pass, you're good to go.

4. (Optional) Download Datasets
For playing with the toolbox alone, I only recommend downloading LibriSpeech/train-clean-100. Extract the contents as <datasets_root>/LibriSpeech/train-clean-100 where <datasets_root> is a directory of your choosing. Other datasets are supported in the toolbox, see here. You're free not to download any dataset, but then you will need your own data as audio files or you will have to record it with the toolbox.

5. Launch the Toolbox
You can then try the toolbox:
python demo_toolbox.py -d <datasets_root>
or
python demo_toolbox.py
depending on whether you downloaded any datasets. If you are running an X-server or if you have the error Aborted (core dumped), see this issue.



Download it here - https://github.com/CorentinJ/Real-Time-Voice-Cloning

Watch the Tutorial Video https://www.youtube.com/watch?v=-O_hYhToKoA

Live, Realtime AI Vishing Scam...

The scam is simple.
Step1 - target a company and map out its corporate hierarchy.

Step 2 - Pick a manager with budgetary authority and, while posing as their company's chief executive.

Step 3 - Email them to say you've agreed a large purchase order, but you need the funds by end of play today.

Step 4 - Before they have a chance to reply, call them up and repeat the message but this time, in the voice of their CEO. "I need the funds yesterday," you tell them. "Can you make that happen?"

UK & US Response to Deepfake Technology

Under a planned amendment to the Online Safety Bill, people who share so-called 'deepfakes' – explicit images or videos which have been manipulated to look like someone without their consent – will be among those to be specifically criminalised for the first time and face potential time behind bars.

In November 2022, the UK Government announced plans to make pornographic deepfakes shared online illegal. “Explicit images or videos which have been manipulated to look like someone without their consent,” will be criminalised in a planned amendment to the Online Safety Bill.

S. 2559 would require the Department of Homeland Security (DHS) to establish a task force to address digital content forgeries, also known as “deepfakes.” These forgeries manipulate digital content, such as videos, with the intent to mislead the viewer.

The task force would investigate the feasibility of deploying standards and technologies for verifying the origin and history of digital content. This is to combat the illegal use of DeepFake technology for propaganda purposes and to defend national security interests.

Thank you for listening.

Remember, know your enemy…