

**FORTRA**™

# Operation Ringing Rascal

Setting up your own social engineering infrastructure

Kyle Gaertner

# What this talk is about

- Bio
- How this project started
- Setting it up
- Legal stuff
- The payoff
- What's next?

# /usr/bin/whoami

- **Kyle Gaertner**
- **Pentester wrangler with Fortra's Digital Defense**
- **CISSP, OSCP, OSWP, CRYPTO, GPEN, GWAPT, GAWN, CEH, CCNA, MCSA, LMNOP, and the alphabet soup goes on...**
- **MS and BS from WGU**
- **Pentesting for 7 years**
- **Other IT for 6 years**
- **Former welder**



## How this project started

- Phone system migration
- Boredom
- Bsides
- What if?

## The phases

- AWS
- SIP Trunk
- FreePBX
- Voice Mod

## AWS

- EC2
- AWS FreePBX
- t2.small (could go smaller)
- Security Groups!

# AWS crash course 1



EC2

The screenshot shows the AWS EC2 Dashboard. On the left, a sidebar menu includes 'New EC2 Experience' (with a feedback link), 'EC2 Dashboard', 'EC2 Global View', 'Events', 'Limits', 'Instances' (selected and highlighted with a red box), 'Instance Types', 'Launch Templates', 'Spot Requests', 'Savings Plans', 'Reserved Instances', 'Dedicated Hosts', 'Scheduled Instances', 'Capacity Reservations', and 'Images'. The main content area is titled 'Resources' and displays a summary of resources in the 'US East (N. Virginia) Region':

Instances (running)	0	Auto Scaling Groups	0
Instances	7	Key pairs	5
Security groups	8	Snapshots	0

Below this, a callout box says: 'Easily size, configure, and deploy Microsoft SQL Server Always On availability groups on AWS using the AW...'.

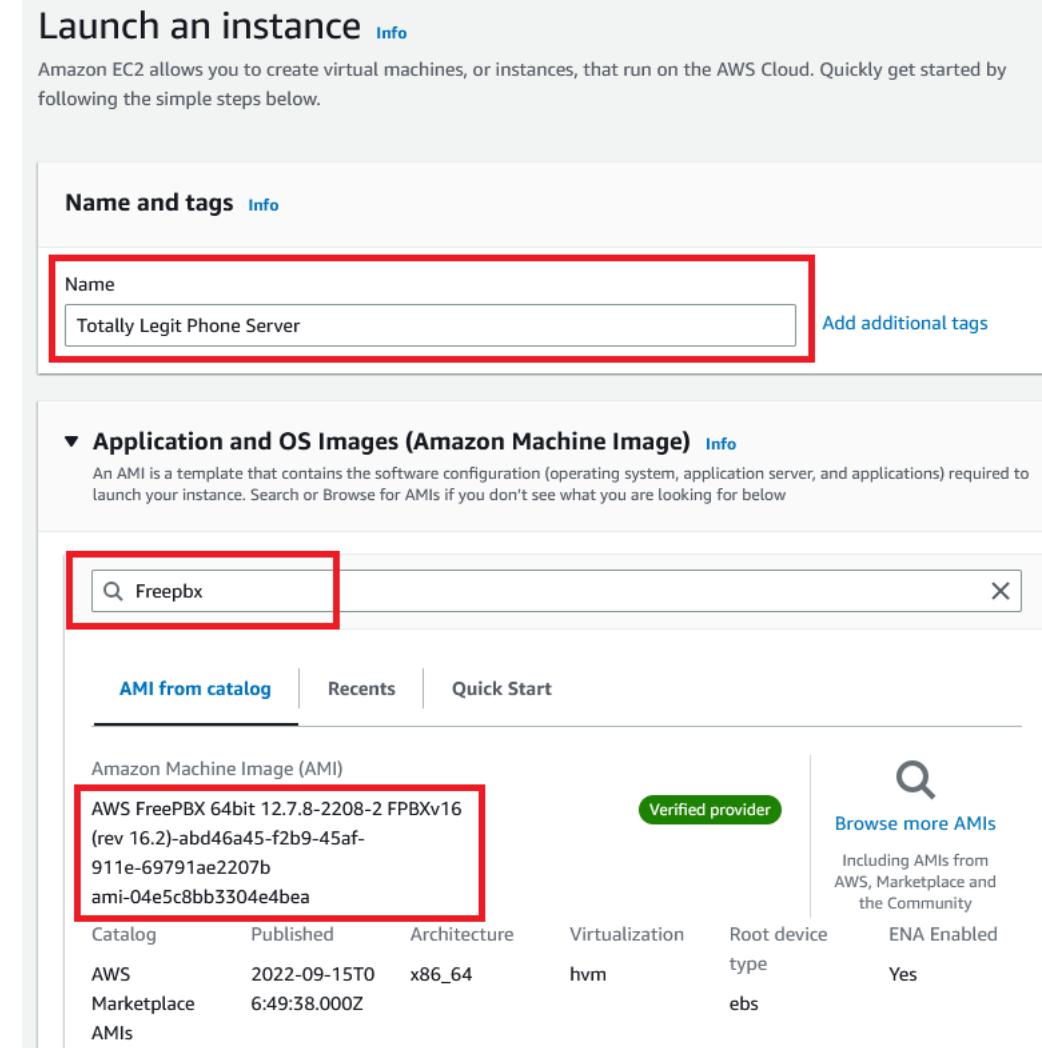
The 'Launch instance' section contains a large yellow button labeled 'Launch instance ▾' (with a red box around it) and a smaller button labeled 'Migrate a server'.

At the bottom, a note states: 'Note: Your instances will launch in the US East (N. Virginia) Region'.



AWS Services Search [Alt+S] Instances (7) Info N. Virginia ▾ Kyle ▾ Tell us what you think Launch Instances

# AWS crash course 2



Launch an instance [Info](#)

Amazon EC2 allows you to create virtual machines, or instances, that run on the AWS Cloud. Quickly get started by following the simple steps below.

Name and tags [Info](#)

Name [Add additional tags](#)

Totally Legit Phone Server

▼ Application and OS Images (Amazon Machine Image) [Info](#)

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. Search or Browse for AMIs if you don't see what you are looking for below

AMI from catalog Recents Quick Start

Search: Freepbx

Amazon Machine Image (AMI)

AWS FreePBX 64bit 12.7.8-22082 FPBxv16  
(rev 16.2)-abd46a45-f2b9-45af-  
911e-69791ae2207b  
ami-04e5c8bb3304e4bea

Verified provider

Catalog Published Architecture Virtualization Root device ENA Enabled

AWS 2022-09-15T0 x86\_64 hvm type Yes

Marketplace 6:49:38.000Z AMIs ebs

Browse more AMIs

Including AMIs from AWS, Marketplace and the Community

# AWS crash course 3

▼ Key pair (login) [Info](#)

You can use a key pair to securely connect to your instance. Ensure that you have access to the selected key pair before you launch the instance.

Key pair name - required

Select

[Create new key pair](#)

▼ Instance type [Info](#)

Instance type

c6a.large

Family: c6a 2 vCPU 4 GiB Memory Current generation: true

Create key pair X

Key pairs allow you to connect to your instance securely.

Enter the name of the key pair below. When prompted, store the private key in a secure and accessible location on your computer. **You will need it later to connect to your instance.** [Learn more](#)

Key pair name

testrgv

The name can include up to 255 ASCII characters. It can't include leading or trailing spaces.

Key pair type

RSA

RSA encrypted private and public key pair

ED25519

ED25519 encrypted private and public key pair (Not supported for Windows instances)

Private key file format

.pem

For use with OpenSSH

.ppk

For use with PuTTY

Cancel

Create key pair

# AWS crash course 4

## Firewall (security groups) Info

A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.

Create security group

Select existing security group

We'll create a new security group called '**AWS FreePBX v16 with included Technical Support-16.2-AutogenByAWSMP--1**' with the following rules:

- |   |                       |
|---|-----------------------|
| <input checked="" type="checkbox"/> Allow SSH traffic from<br>Recommended rule from AMI   | Anywhere<br>0.0.0.0/0 |
| <input checked="" type="checkbox"/> Allow CUSTOMTCP traffic from<br>Recommended rule from AMI   | Anywhere<br>0.0.0.0/0 |
| <input checked="" type="checkbox"/> Allow CUSTOMUDP traffic from<br>Recommended rule from AMI   | Anywhere<br>0.0.0.0/0 |
| <input checked="" type="checkbox"/> Allow CUSTOMUDP traffic from<br>Recommended rule from AMI   | Anywhere<br>0.0.0.0/0 |
| <input checked="" type="checkbox"/> Allow CUSTOMUDP traffic from<br>Recommended rule from AMI   | Anywhere<br>0.0.0.0/0 |
| <input checked="" type="checkbox"/> Allow CUSTOMTCP traffic from<br>Recommended rule from AMI   | Anywhere<br>0.0.0.0/0 |
| <input checked="" type="checkbox"/> Allow CUSTOMUDP traffic from<br>Recommended rule from AMI   | Anywhere<br>0.0.0.0/0 |
| <input checked="" type="checkbox"/> Allow CUSTOMTCP traffic from<br>Recommended rule from AMI   | Anywhere<br>0.0.0.0/0 |
| <input checked="" type="checkbox"/> Allow CUSTOMTCP traffic from<br>Recommended rule from AMI   | Anywhere<br>0.0.0.0/0 |
| <input checked="" type="checkbox"/> Allow CUSTOMTCP traffic from<br>Recommended rule from AMI   | Anywhere<br>0.0.0.0/0 |
| <input checked="" type="checkbox"/> Allow HTTPS traffic from the internet<br><small>To set up an endpoint, for example when creating a web server</small> | Anywhere<br>0.0.0.0/0 |
| <input type="checkbox"/> Allow HTTP traffic from the internet<br><small>To set up an endpoint, for example when creating a web server</small>             | Anywhere<br>0.0.0.0/0 |

**⚠️** Rules with source of 0.0.0.0/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only. X

# AWS crash course 5

## Edit inbound rules Info

Inbound rules control the incoming traffic that's allowed to reach the instance.

Inbound rules <small>Info</small>						
Security group rule ID	Type <small>Info</small>	Protocol <small>Info</small>	Port range <small>Info</small>	Source <small>Info</small>	Description - optional <small>Info</small>	
sgr-[REDACTED]	Custom UDP	UDP	10000 - 64000	Custom	questblue (sip trunk)	<button>Delete</button>
sgr-[REDACTED]a	Custom UDP	UDP	10000 - 20000	Custom	[REDACTED]e - voice portion	<button>Delete</button>
sgr-[REDACTED]	SSH	TCP	22	Custom	ssh - [REDACTED]	<button>Delete</button>
sgr-[REDACTED]e	Custom UDP	UDP	5060	Custom	[REDACTED] - chan_sip signaling	<button>Delete</button>
sgr-[REDACTED]5	HTTPS	TCP	443	Custom	[REDACTED] - https	<button>Delete</button>

# AWS crash course 6

Instances (2) [Info](#)

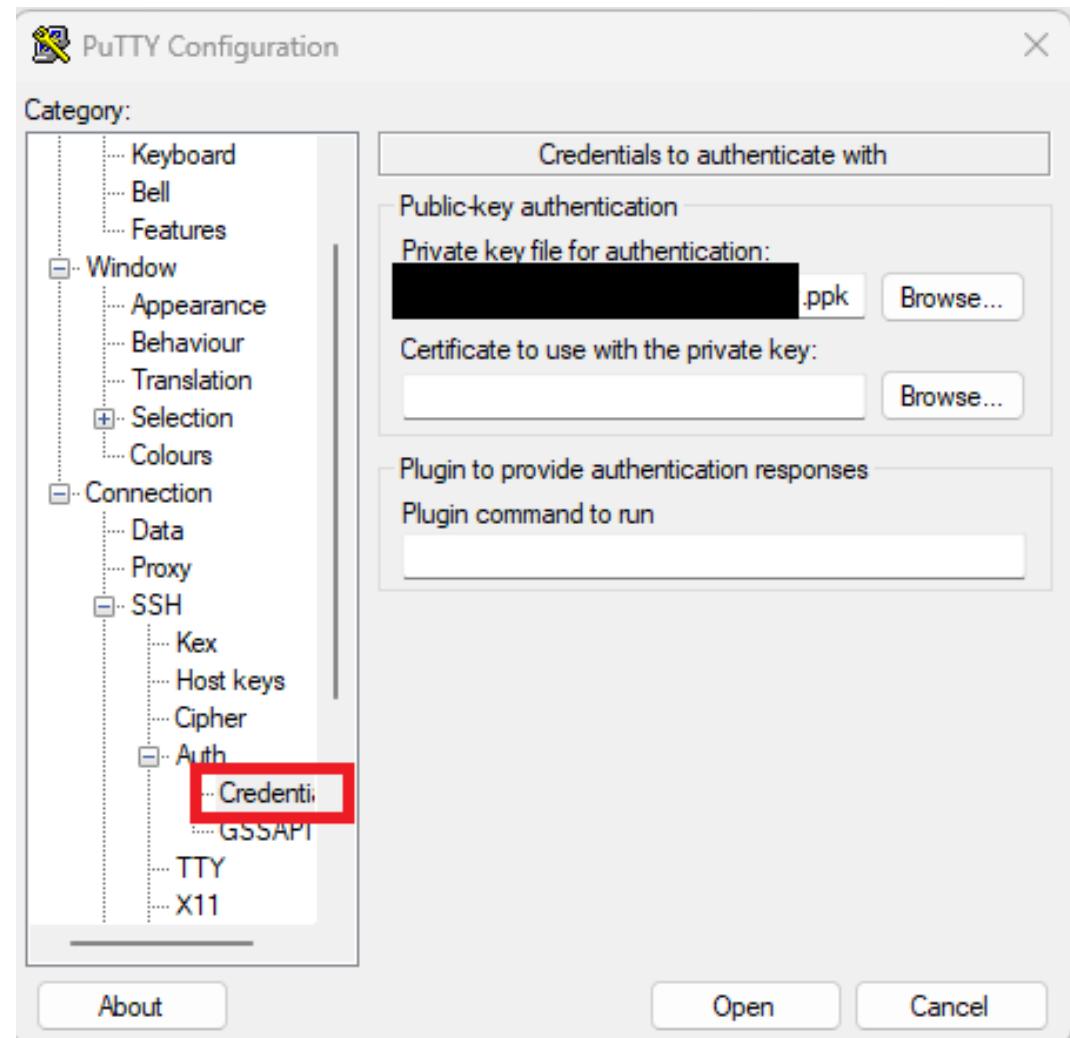
Connect [Instance state ▾](#) [Actions ▾](#) [Launch instances](#) ▾

Find instance by attribute or tag (case-sensitive) < 1 > ⚙️

[rgv](#) [X](#) | [Clear filters](#)

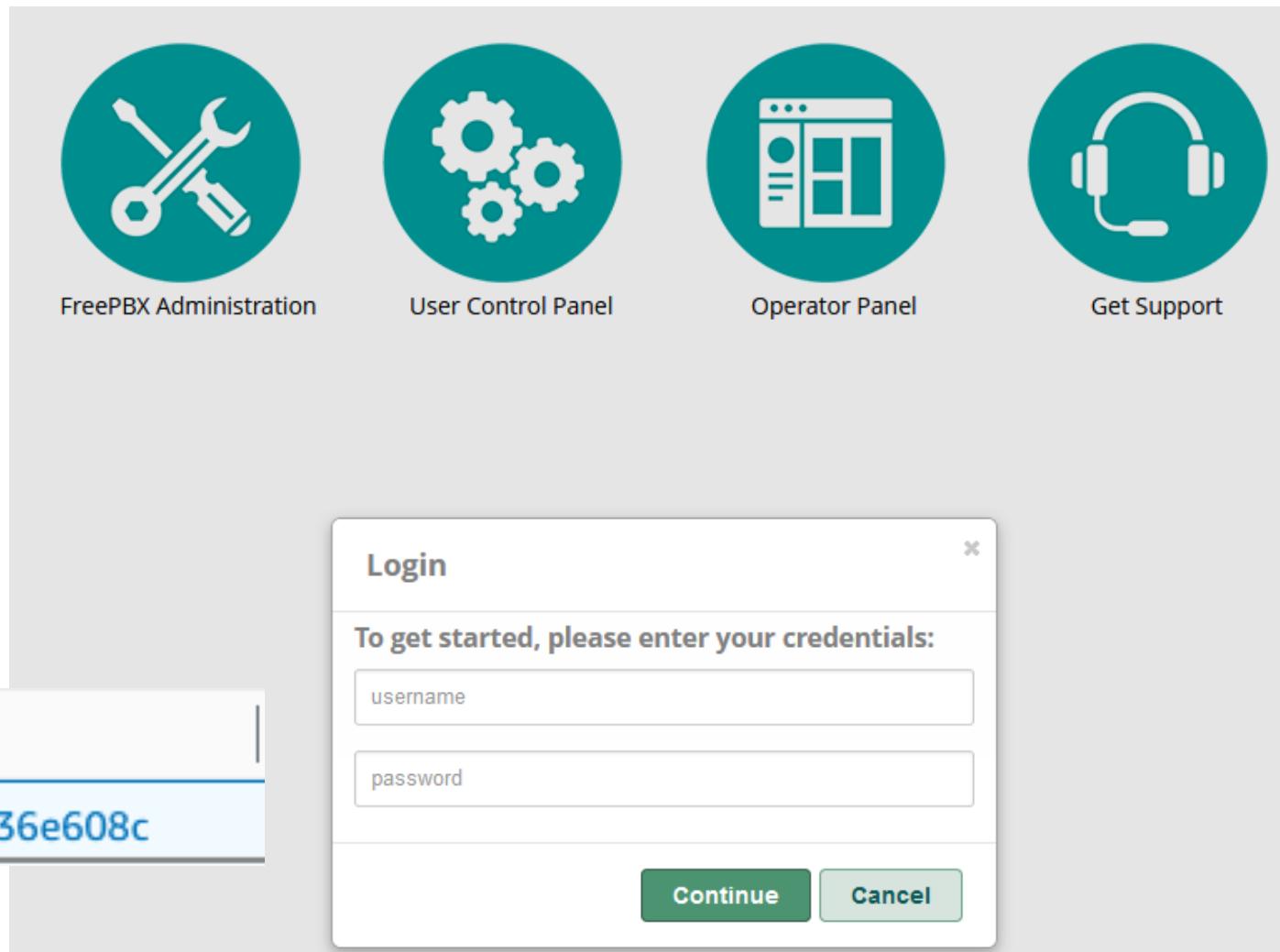
<input type="checkbox"/>	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS	Public IPv4
<input type="checkbox"/>	rgv <a href="#">✍️</a>	i-02982b3de136e608c	<a href="#">Running</a> <a href="#">🕒</a>	t2.small	<a href="#">2/2 checks passed</a>	No alarms <a href="#">+</a>	us-east-1b	ec2-18-206-188-100.co...	18.206.188.

# AWS crash course 7



# AWS crash course 8

<input checked="" type="checkbox"/>	Name	Instance ID
<input checked="" type="checkbox"/>	rgv	i-02982b3de136e608c



# AWS crash course 9

# SIP Trunk 1

The screenshot shows the QUESTBLUE web application interface. At the top, the logo "QUESTBLUE™" is displayed in white on a blue header bar. Below the header, a welcome message "Welcome Kyle Gaertner" and a balance of "\$47.48" are shown. A dropdown arrow is positioned next to the balance.

The left sidebar, titled "Main", contains the following navigation items:

- Dashboard** (selected, highlighted in blue)
- Additional Services
- Asset Management
- LNP
- Messaging
- Reports
- SIP Trunks
- Servers
- Support
- Telephone Numbers

Below the sidebar, there are two buttons: "Offnet E911" and "Order Telephone Numbers".

The right panel is titled "Order TNs" and features a "Search" button in a green box. Below it are two tabs: "Regular" (highlighted in blue) and "Toll-Free".

Underneath the tabs, there is a "Search By:" section with radio buttons for "State/City", "Zip", "WildCard", and "Area Code". The "Area Code" option is selected. To the right of this section is a search input field labeled "Area Code" with a clear icon, and a "More Options" link at the bottom.

## SIP Trunk 2

**Create Trunk**

Trunk Name

Trunk Type  
 Static IP Trunk

IP Address

Trunk Region  
 United States    Domain: sbc.questblue.com

Max Channels  
 ▲ ▼

**Create Trunk**

# SIP Trunk 3

Siptrunks						
Type to search						
TRUNK TYPE	SIP NAME	IP ADDRESS	CREATION DATE	INTERNATIONAL	CONNECTION	STATUS
Static	new1234	54.242.163.21	2/20/2020, 10:26:18 PM	Inactive	N/A	Active

# FreePBX 1

- **Connectivity \ Trunks**

**Apply Config**

The screenshot shows the FreePBX Trunk configuration interface. It includes tabs for General, Dial Number Manipulation Rules, and sip Settings.

**General Tab:**

- Trunk Name:** new1234

**Dial Number Manipulation Rules Tab:**

- Rules:**
  - X matches any digit from 0-9
  - Z matches any digit from 1-9
  - N matches any digit from 2-9
  - [1237-9] matches any digit or letter in the brackets (in this example, 1,2,3,7,8,9)
  - . wildcard, matches one or more characters (not allowed before a | or +)
- Two examples of manipulation rules are shown:
  - ( 1 ) prefix | [ NXXNXXXXX
  - ( prepend ) prefix | [ 1NXXNXXXXX

**sip Settings Tab:**

```

new1234

type=peer
host=sbc.questblue.com
insecure=very
context=from-trunk
qualify=yes
nat=no
session-timers=refuse
  
```

**Outgoing Tab:**

- USER Context:** from-trunk
- USER Details:** type=peer&from-trunk

# FreePBX 2

- **Connectivity \ Inbound Routes**

General	Advanced	Privacy	Fax	Other
Description ?	inbound			
DID Number ?	2109104557			
CallerID Number ?	ANY			
CID Priority Route ?	<input checked="" type="button"/> Yes <input type="button"/> No			
Alert Info ?	None			
Ringer Volume Override ?	None			
CID name prefix ?				
Music On Hold ?	Default			
Set Destination ?	Extensions 1000 1000			

# FreePBX 3

- Connectivity \ Outbound Routes

Route Settings   Dial Patterns   Import/Export Patterns   Notifications

Dial Patterns that will use this Route

Pattern Help

( prepend ) prefix | [ 1NXXNXXXXX ]

( 1 ) prefix | [ NXXNXXXXX ]

Route Settings   Dial Patterns   Import/Export Patterns   Notifications

**Route Name** ?

**Route CID** ?

**Override Extension** ?  Yes  No

**Route Password** ?

**Route Type** ?  Emergency  Internal

**Music On Hold?** ?

**Time Match Time Zone:** ?

**Time Match Time Group** ?

**Trunk Sequence for Matched Routes** ?

# FreePBX 4

- **Settings \ Asterisk SIP Settings**

General SIP Settings    SIP Legacy Settings [chan\_sip]

Other SIP Settings ?

session-timers = refuse 1

General SIP Settings    SIP Legacy Settings [chan\_sip]

—Security Settings

Allow Anonymous Inbound SIP Calls ?    Yes    No

Allow SIP Guests ?    Yes    No

Default TLS Port Assignment ?    Chan SIP    PJSip

—NAT Settings

External Address ?    54.242.163.21

Detect Network Settings

# FreePBX 5

- Applications \ Extensions

Extension: 1000

General

Voicemail

Find Me/Follow Me

Advanced

Pin Sets

Other

## — Edit Extension

This device uses **CHAN\_SIP** technology listening on Port 5060 (UDP)

Display Name 

1000

Outbound CID 

(956) 555-1234

Emergency CID 

[redacted]

Secret 

[redacted]

# FreePBX 6

- Admin \ User Management

## Edit User

FreePBX Administration GUI

Contact Manager

Login Details    User Details    Advanced    FreePBX Administration GUI    Contact Manager

Login Name ?	1000
Description ?	Autogenerated user on new device creation
Password ?	*****
Groups ?	All selected (1) ▾
Primary Linked Extension ?	1000 <1000> ▾

User Details    Advanced    FreePBX Administration GUI

Login Details    User Details    Advanced    FreePBX Administration GUI    Contact Manager

First Name ?	
Last Name ?	
Display Name ?	(956) 555-1234

# Linphone



## ACCOUNT ASSISTANT

Create or manage your Linphone account.

ASSISTANT

USE A SIP ACCOUNT

## USE A SIP ACCOUNT

Username

Display name (optional)

SIP Domain

Password

Transport

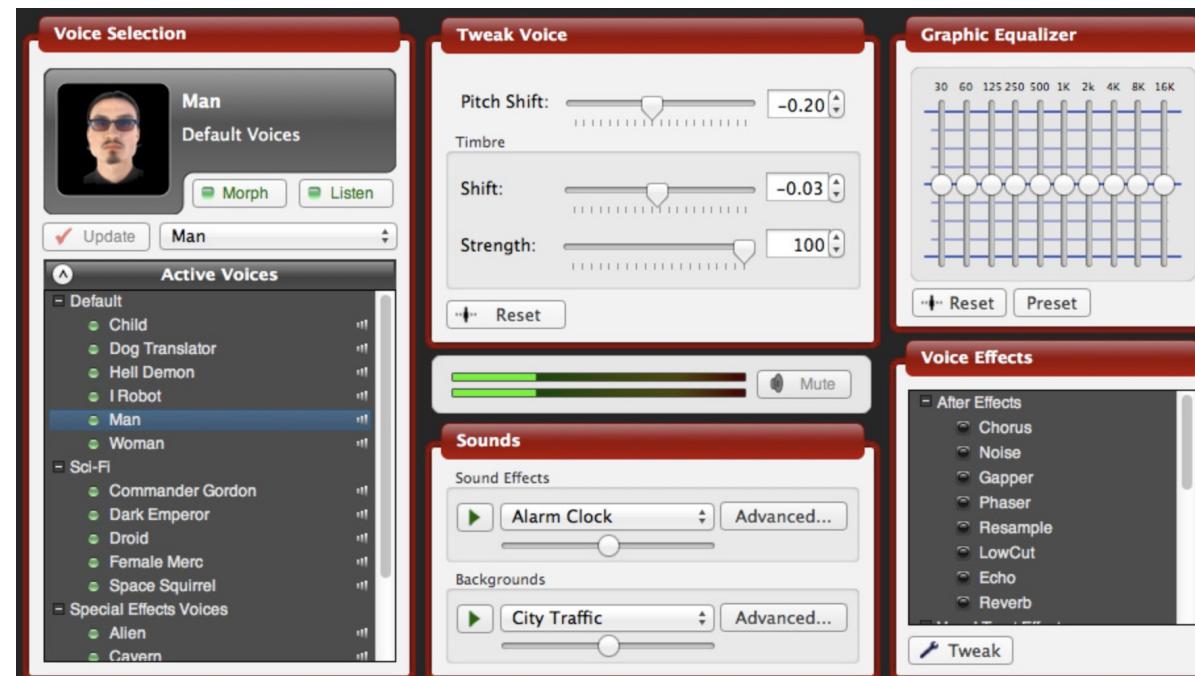
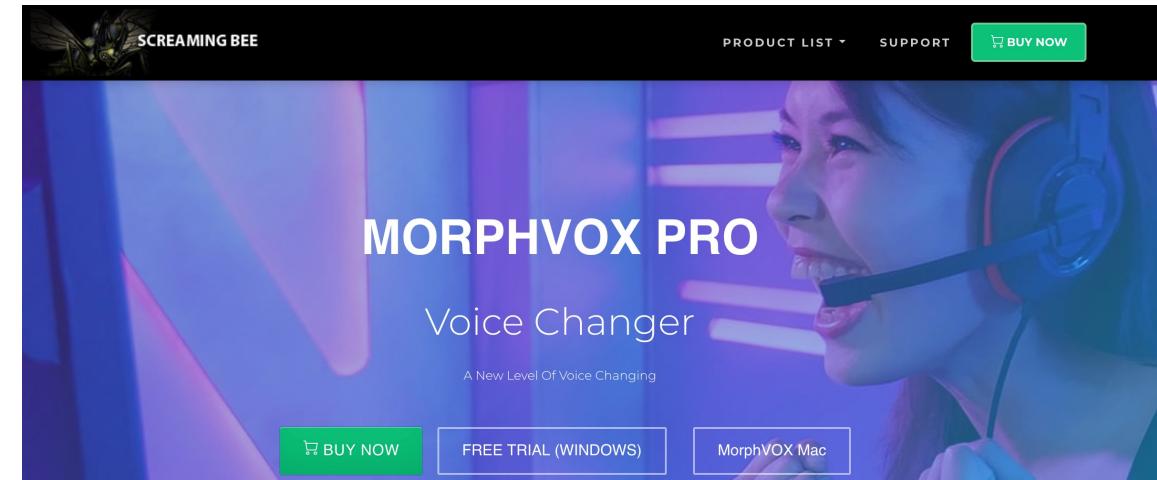
UDP

BACK

USE

# Voice Mod

- Voice Packs
- Backgrounds



## Legal Stuff

- **Truth in Caller ID Act of 2009**
- **STIR/SHAKEN**

# Truth in Caller ID Act of 2009

- “**Truth in Caller ID Act of 2009 - Amends the Communications Act of 1934 to make it unlawful for any person in the United States, in connection with any telecommunications service or Internet protocol (IP)-enabled voice service, to cause any caller identification (ID) service to transmit misleading or inaccurate caller ID information with the intent to defraud, cause harm, or wrongfully obtain anything of value, unless such transmission is exempted in connection with: (1) authorized activities of law enforcement agencies; or (2) a court order specifically authorizing the use of caller ID manipulation.**”

\*<https://www.congress.gov/bill/111th-congress/senate-bill/30>

- **Fines up to \$10,000**

# STIR/SHAKEN

- **STIR/SHAKEN is a framework of interconnected standards.**  
STIR/SHAKEN are acronyms for the Secure Telephone Identity Revisited (STIR) and Signature-based Handling of Asserted Information Using toKENs (SHAKEN) standards. This means that calls traveling through interconnected phone networks can have their caller ID "signed" as legitimate by originating carriers and validated by other carriers before reaching consumers.  
STIR/SHAKEN digitally validates the handoff of phone calls passing through the complex web of networks, allowing the phone company of the consumer receiving the call to verify that a call is in fact from the number displayed on Caller ID.
- **tl;dr: certificate authorities, verification, trusts, fines**

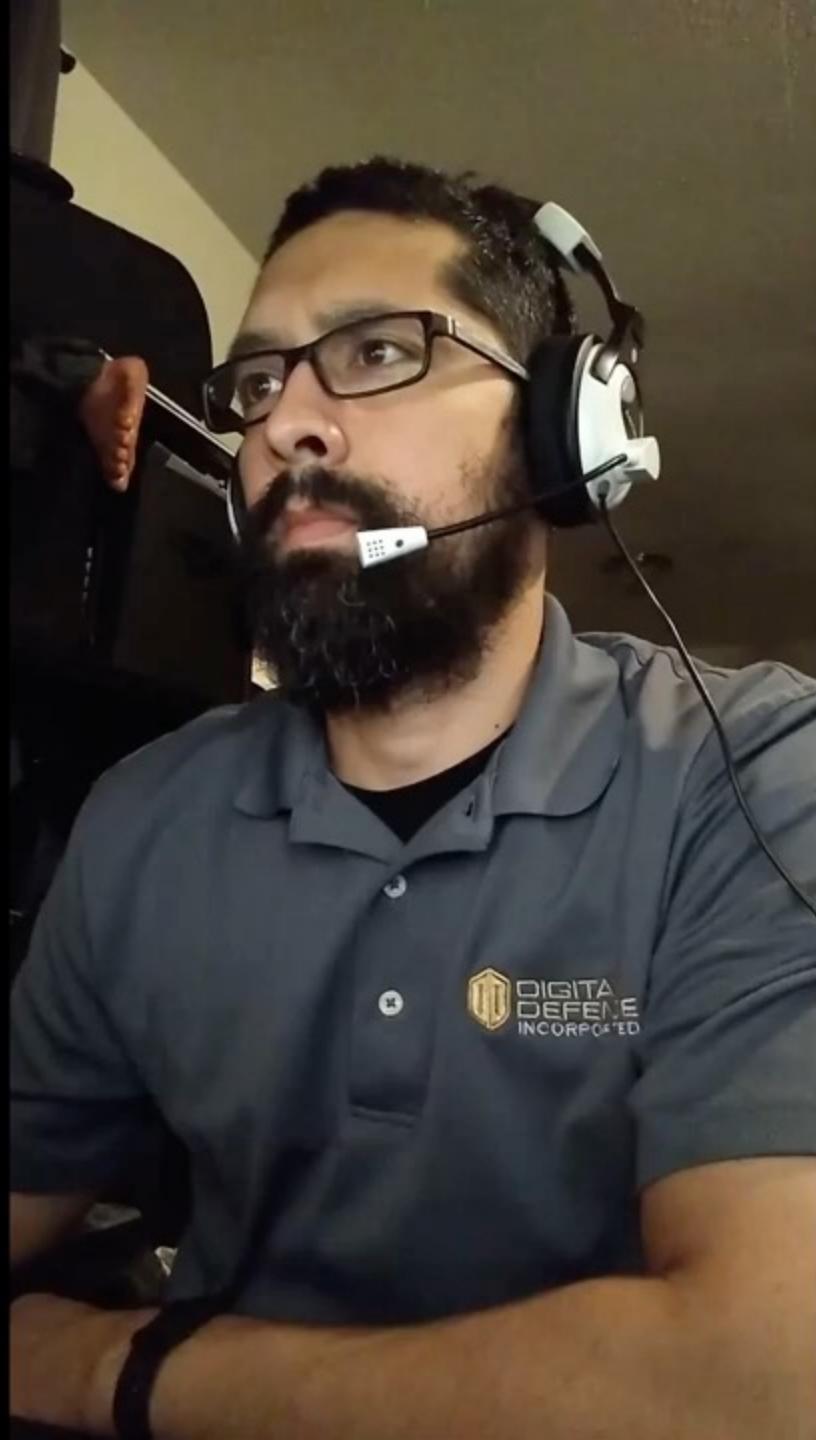
\*<https://www.fcc.gov/call-authentication>

# It works? It works!

- **Convincing premise?**
- **Emotional response**
- **Pressure**









## The payoff

- Is my face red?
- Solved a few problems
- Had a few laughs

## What's this talk really about?

- **Nothing groundbreaking**
- **Based on the work of others**

## Credits

Jonathan Stines - <https://www.rapid7.com/blog/post/2018/05/24/how-to-build-your-own-caller-id-spoofing-part-1/>

Ventz - <https://blog.vpetkov.net/2011/07/10/spoofing-caller-id-on-the-fly-from-any-phone-for-legal-and-legitimate-purposes/>

# Questions

[kyle.gaertner@fortra.com](mailto:kyle.gaertner@fortra.com)

@unskilledk

[\*\*https://github.com/unskilledk/slides/2023RGV\*\*](https://github.com/unskilledk/slides/2023RGV)