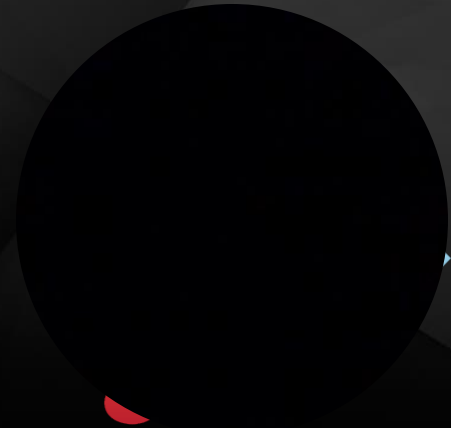


**This slide deck is from a security presentation by Steve Stasiukonis from SNT. If you would like to schedule a live web presentation of this material, please reach out to**

**Jim Ockenden  
(315) 949-2803**

# PHISHING SMISHING AND VISHING

HOW TO SPOT THE FAKE



# ABOUT THIS TRAINING SESSION

**IDENTIFYING EMAIL PHISHING THREATS**

**IDENTIFYING SMS PHISHING THREATS**

**IDENTIFYING VOICE PHISHING THREATS**

**HOW MALWARE IS TIED TO THESE THREATS**

**STEPS TO COMBAT THE THREATS**

# **INCREASE IN CYBER CRIMES?**

**ALL START WITH A FORM OF  
PHISHING ,VISHING, SMSHING**



**FINANCIAL SCAMS, CONFIDENCE SCHEMES**



**EXTORTION & BLACKMAIL**



**INTELLECTUAL PROPERTY & DATA THEFT**



**RANSOM & EXFILTRATION OF DATA**

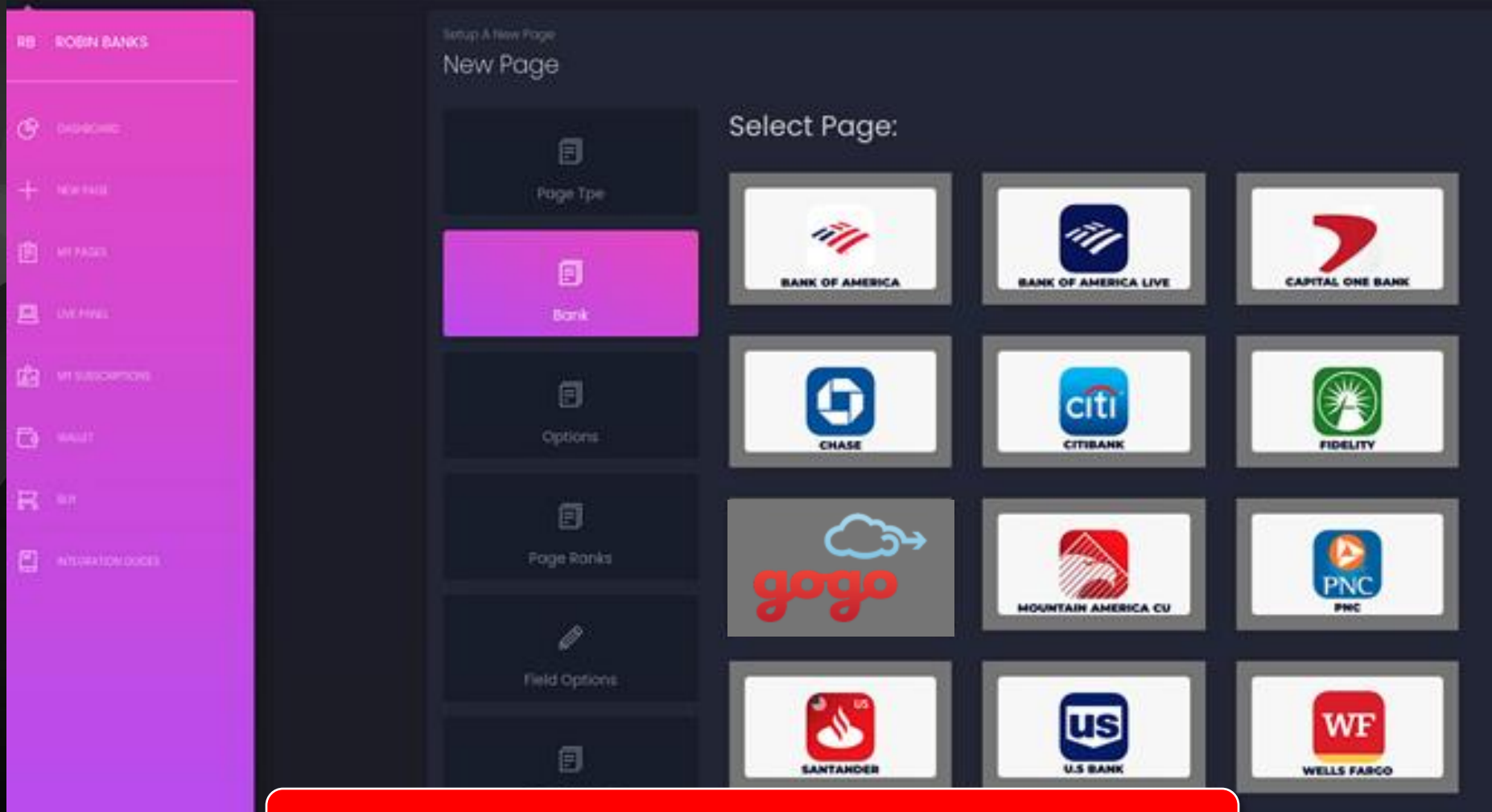


**REDIRECTION OF FUNDS**

# **SPEAR PHISHING AS A SERVICE**

**THREAT ACTORS ARE  
AUTOMATING PHISHING  
EFFORTS**

# PHISHING AS A SERVICE



# USING DARK AI FOR PHISHING AS A SERVICE



## WormGPT

AI Powered Hacking Tool



## WormGPT

AI Powered Hacking Tool

[Home](#)[Pricing](#)[FAQ](#)[Disclaimer](#)[Contact](#)[Login](#)

### WormGPT: The Ultimate Game-changer

Yo, check it out, fam! WormGPT's the real deal, straight outta the hacker's playbook. Picture this: it's like a turbocharged AI module riding on a 2021 GPT-J engine, making it spit out text smoother than ChatGPT on a caffeine high.

But here's the kicker: while OpenAI's holding ChatGPT on a leash, WormGPT's out here running wild and free. No anti-abuse filters, no restrictions—just pure, unadulterated power. You want it to drop some shady lines or cook up a virus? Done and done.

Now, y'all heard about its knack for crafting BEC attacks, right? But lemme tell ya, that's just the tip of the iceberg. WormGPT's packing more tricks up its sleeve than you can shake a USB stick at. Unlimited characters? Check. Memory retention? You got it. And don't even get me started on its coding chops—it's like having a cyber-savvy ninja in your back pocket, ready to whip up some malware mayhem.

But here's the real deal: WormGPT ain't conjuring up anything more mind-bending than a skilled hacker could dream up. Nah, the real power lies in its simplicity and speed. It's like the ultimate hack tool, leveling the playing field so anyone with an internet connection can dive in headfirst.

So, buckle up, folks. With WormGPT on the scene, things are about to get real interesting, real fast.

[Become God](#)

xmva4tp7zgxm...



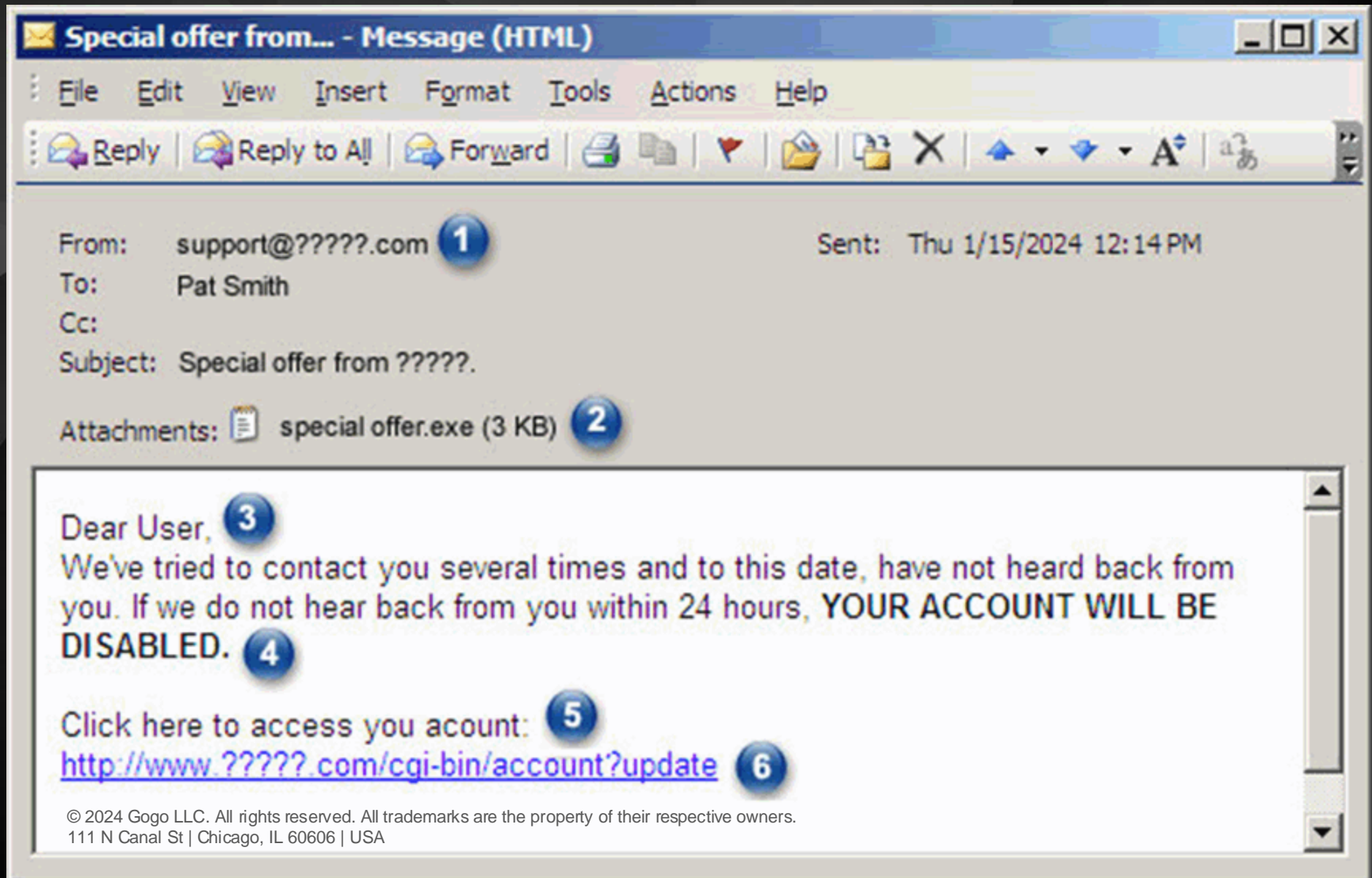
# THE SIMPLE HACKS

PHISHING ,VISHING, SMSHING  
& GETTING YOU TO CLICK.

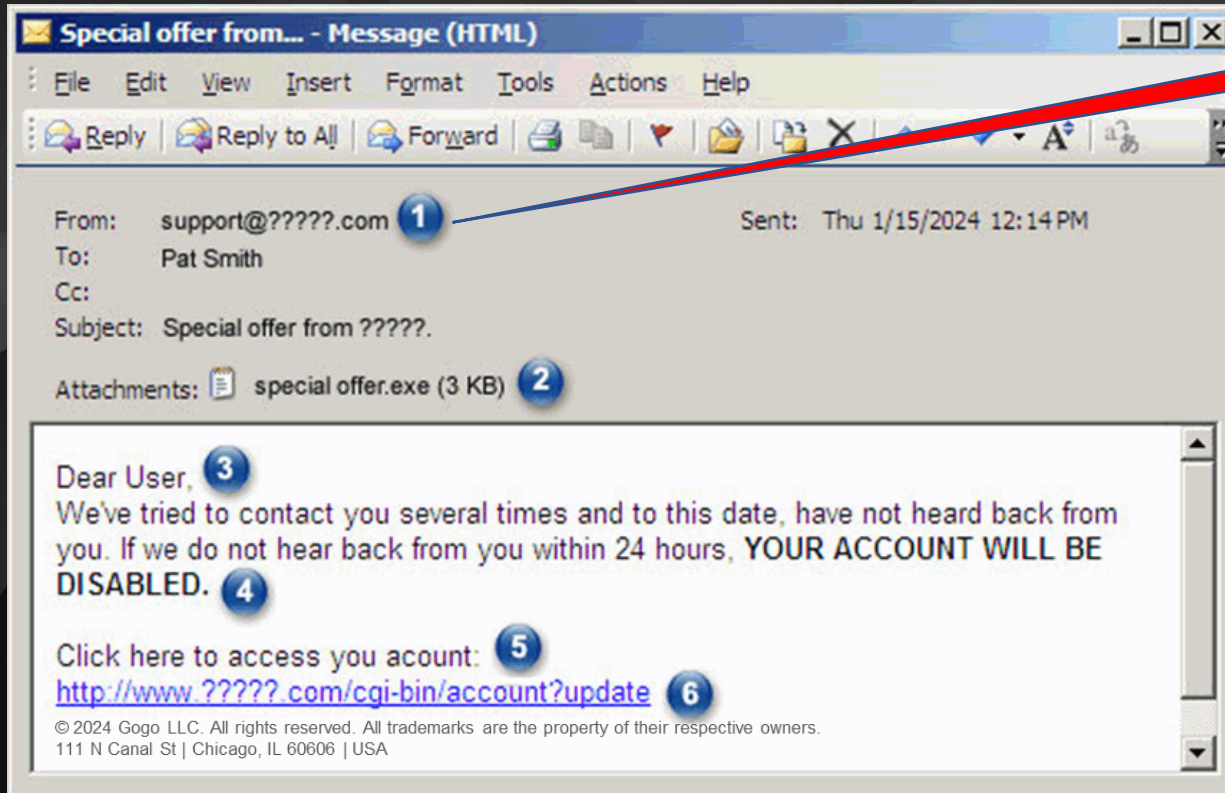
# **EMAIL CREDENTIAL PHISHING**

**HOW TO SPOT THE FAKE**

# SPEAR PHISHING ATTACK VECTOR



# SPEAR PHISHING ATTACK VECTOR



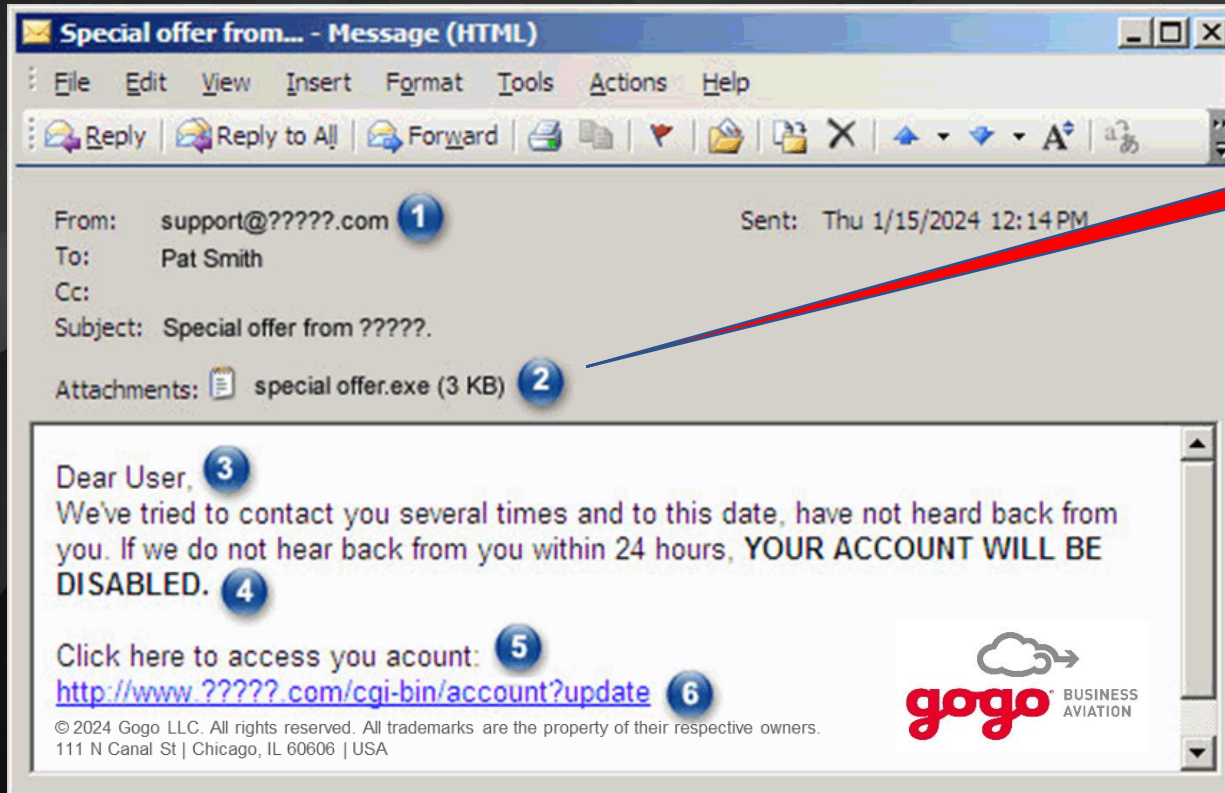
Who Is Sending This?



SUPPORT@ACME.COM

SUPPORT@ACNNE.COM

# SPEAR PHISHING ATTACK VECTOR



If Not Sure. DO NOT  
Open Attachment!

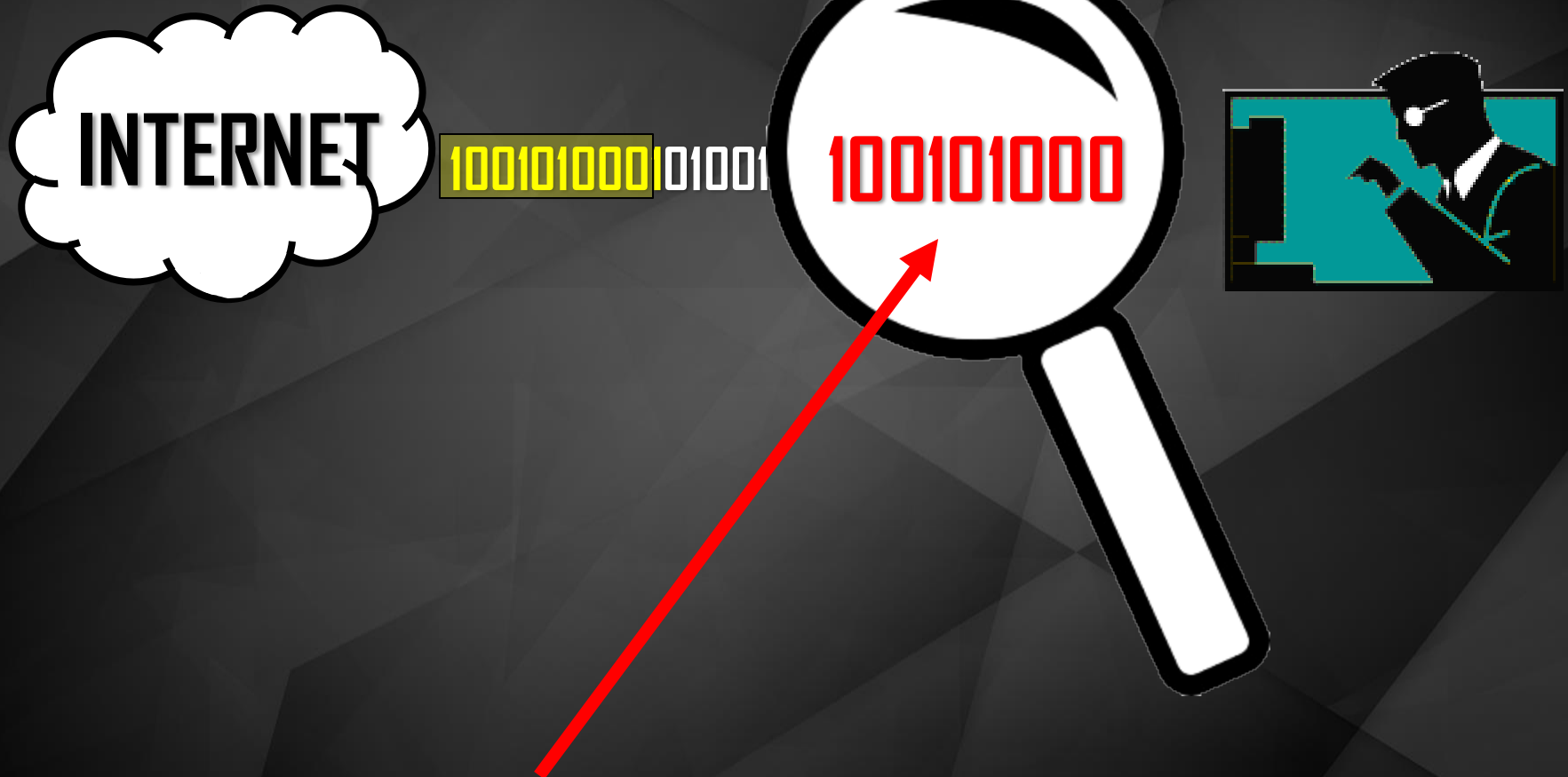


## ANY FILE FORMAT

**EMAIL PHISHING**

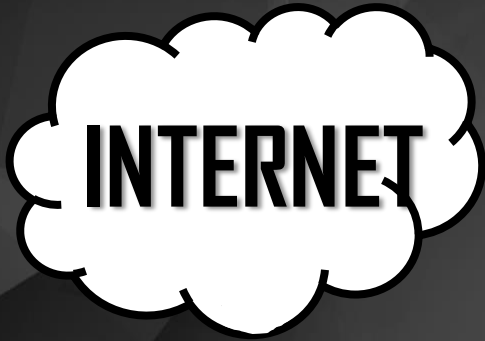
**AND HOW MALWARE  
PLAYS A PART**

# MALWARE-KNOWN VS. ZERO DAY

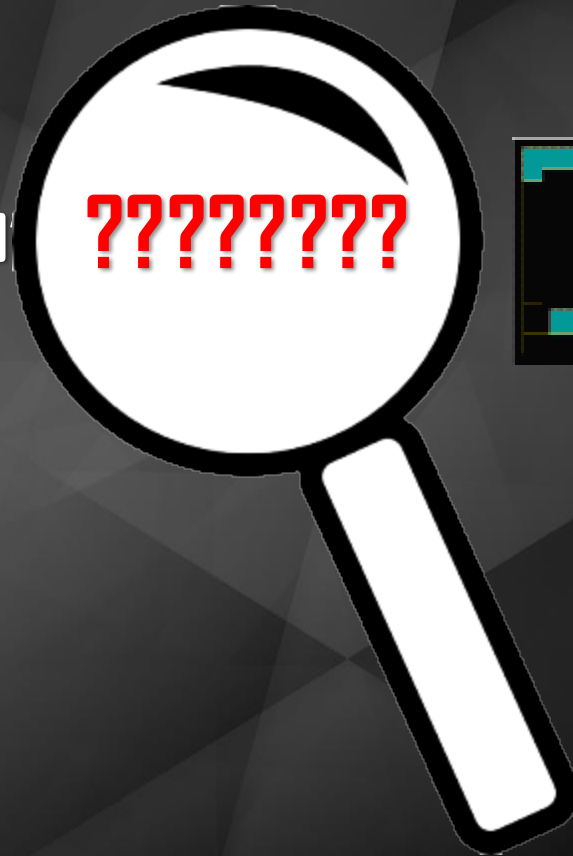


**MATCHES SIGNATURE = SQL SLAMMER**  
**ANTIVIRUS BLOCKS & PROTECTS YOU**

# MALWARE-KNOWN VS. ZERO DAY



00001010100100



**NO SIGNATURE = ZERO DAY**  
**ANTIVIRUS DOES NOT PROTECT YOU**



# MALWARE-HOW IS IT DEPLOYED



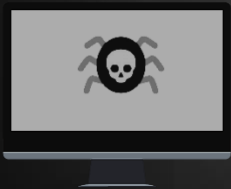
EMAIL ATTACHMENTS, EMBEDDED LINKS & MACROS



WEBSITE DRIVE BY DOWNLOAD



DEPLOYED WITH SOCIAL MEDIA & NETWORKING



EMBEDDED IN HARDWARE DEVICES (i.e. USB)



SOCIAL ENGINEERING

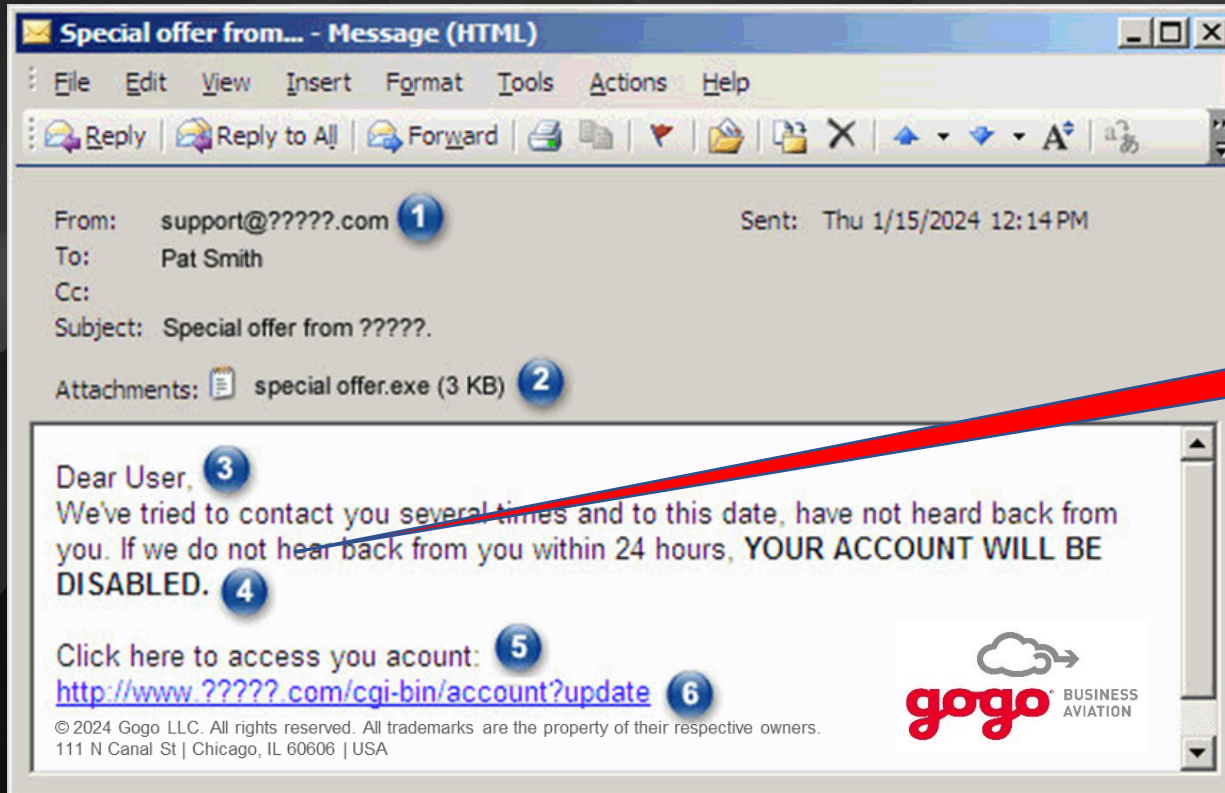


VULNERABLE SYSTEMS

# **EMAIL PHISHING**

**LURING YOU TO AN EVIL TWIN  
WEBSITE**

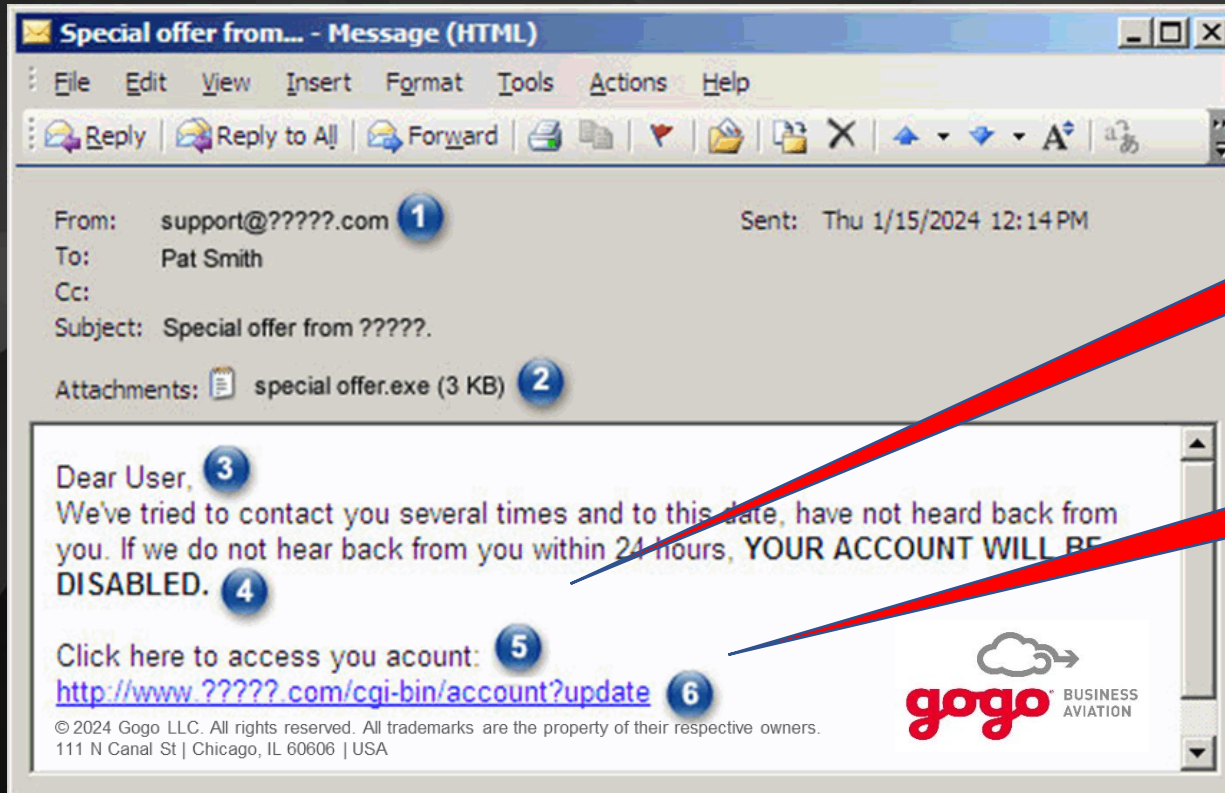
# SPEAR PHISHING ATTACK VECTOR



They Threaten You To  
Do Something

DON'T BE INTIMIDATED

# SPEAR PHISHING ATTACK VECTOR

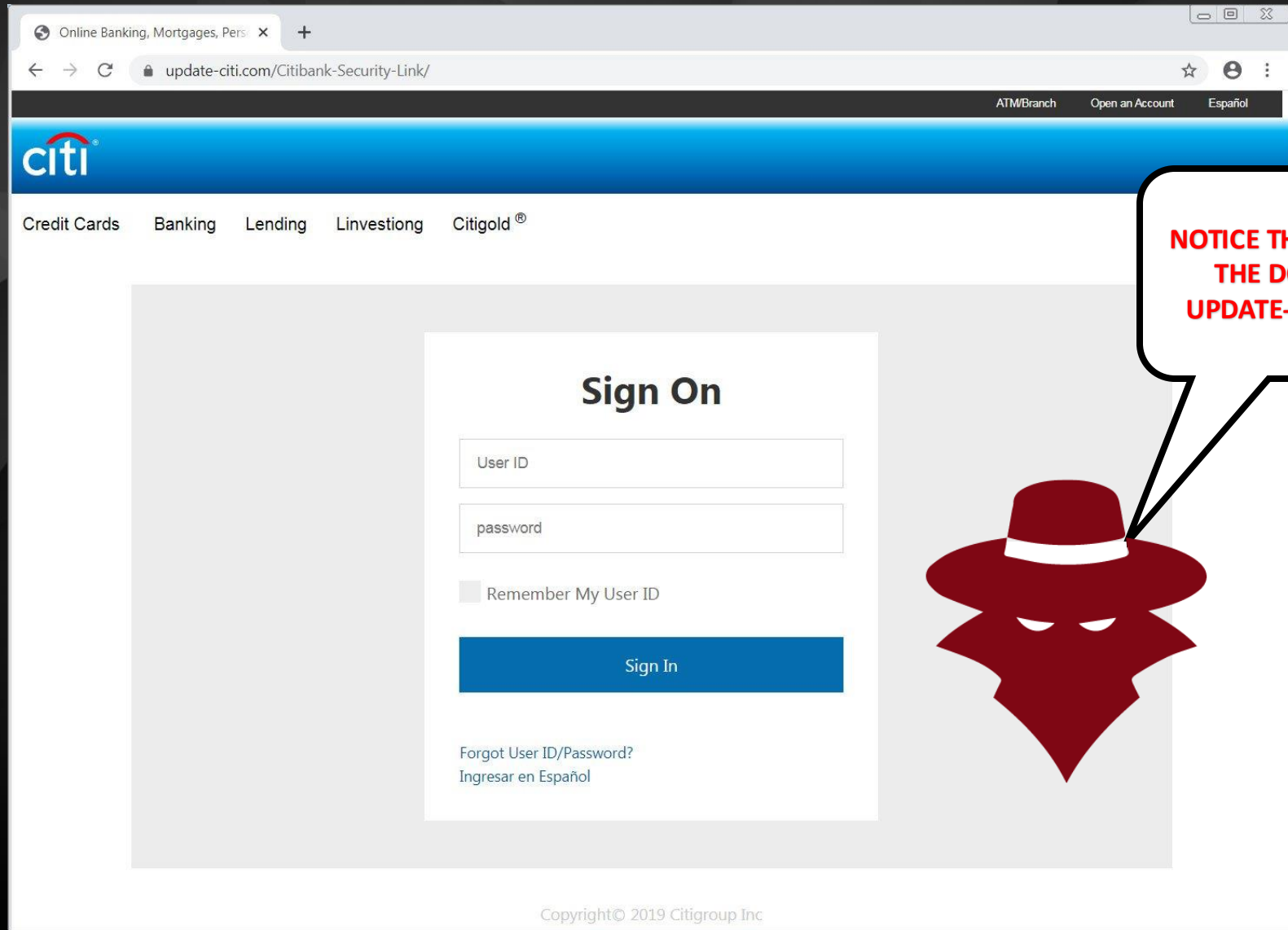


They Instruct You To Do Something?

Hover Over The Link..  
[http://mal+hak-vctm-\\$.br](http://mal+hak-vctm-$.br)

MOUSE HOVERING

# LURED TO EVIL TWIN WEBSITES



# LURED TO EVIL TWIN WEBSITE

Online Banking, Mortgages, Pers × +

← → ↻ [update-citi.com/Citibank-Security-Link/](#)

ATM/Branch Open an Account

**citi**

Credit Cards Banking Lending Linvestment Citigold®

## Sign On

User ID

password

☐ Remember My User ID

Sign In

[Forgot User ID/Password?](#)  
[Ingresar en Español](#)

Copyright© 2019 Citigroup Inc

**THE GOAL IS  
TO COLLECT  
CREDENTIALS**



**TROUBLE  
LOGGING IN?**

**HOW CAN I  
HELP YOU?**



**DOWNLOAD  
THIS FILE**

# CHECKING EVIL TWIN WEBSITES

New Tab

Search Google or type a URL

High Risk Website Blocked: http://update-citi.com

Not secure | update-citi.com

High Risk Website Blocked: http://update-citi.com

Whois update-citi.com

whois.com/whois/update-citi.com

BLACKFRIDAY SALE Get a FREE .FOUNDATION or .GIVES with any domain purchase Coupon: BFCM2022

Whois Identity for everyone

Enter Domain or IP WHOIS

DOMAINS WEBSITE CLOUD HOSTING SERVERS EMAIL SECURITY WHOIS SUPPORT LOGIN

update-citi.com Updated 1 second ago Interested in similar domains?

Domain Information	
Domain:	update-citi.com
Registrar:	DYNADOT, LLC
Registered On:	2022-06-05
Expires On:	2023-06-05
Updated On:	2022-06-05
Status:	ok
Name Servers:	170.ns1.above.com 170.ns2.above.com

Registrant Contact

Email: <https://www.dynadot.com/domain/contact-request?domain=update-citi.com>

updatesciti.com Buy Now

updateciti.com Buy Now

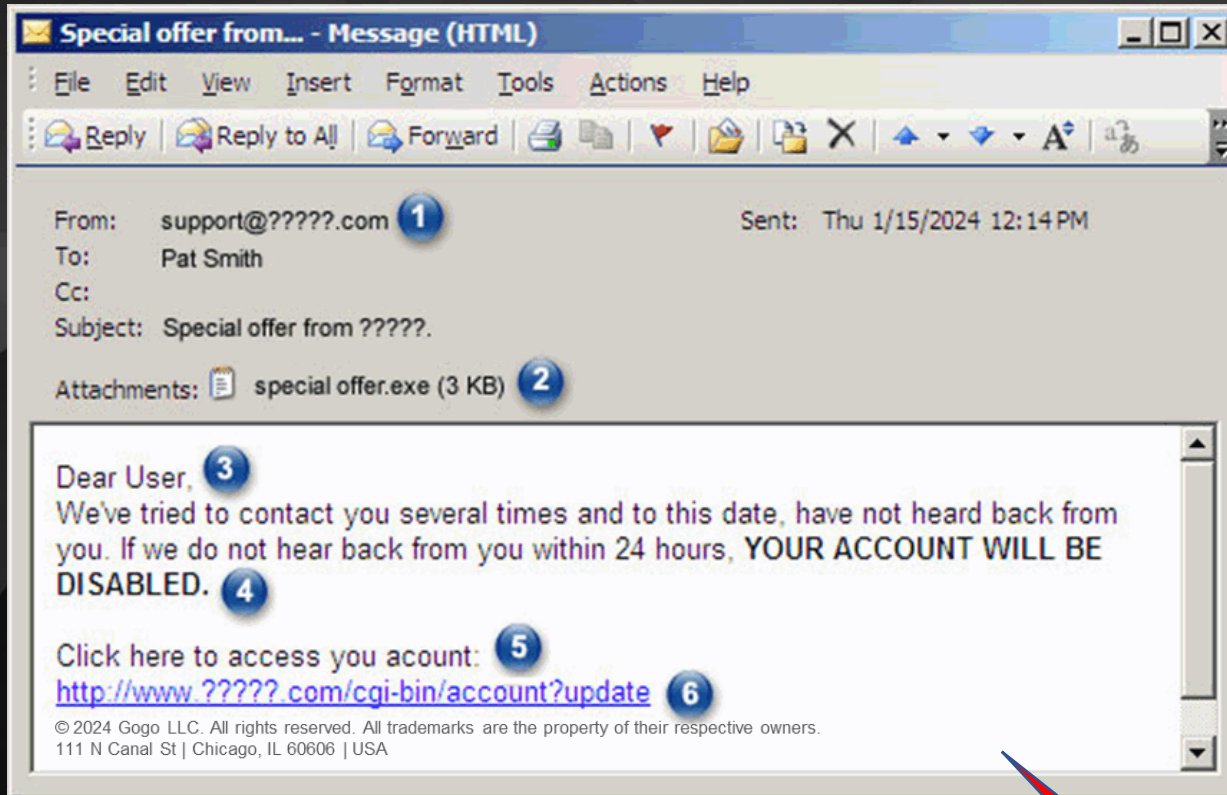
.space \$24.88 \$0.88 BUY NOW

\*Offer ends 30th November 2022

**NOT SURE ASK I.T**



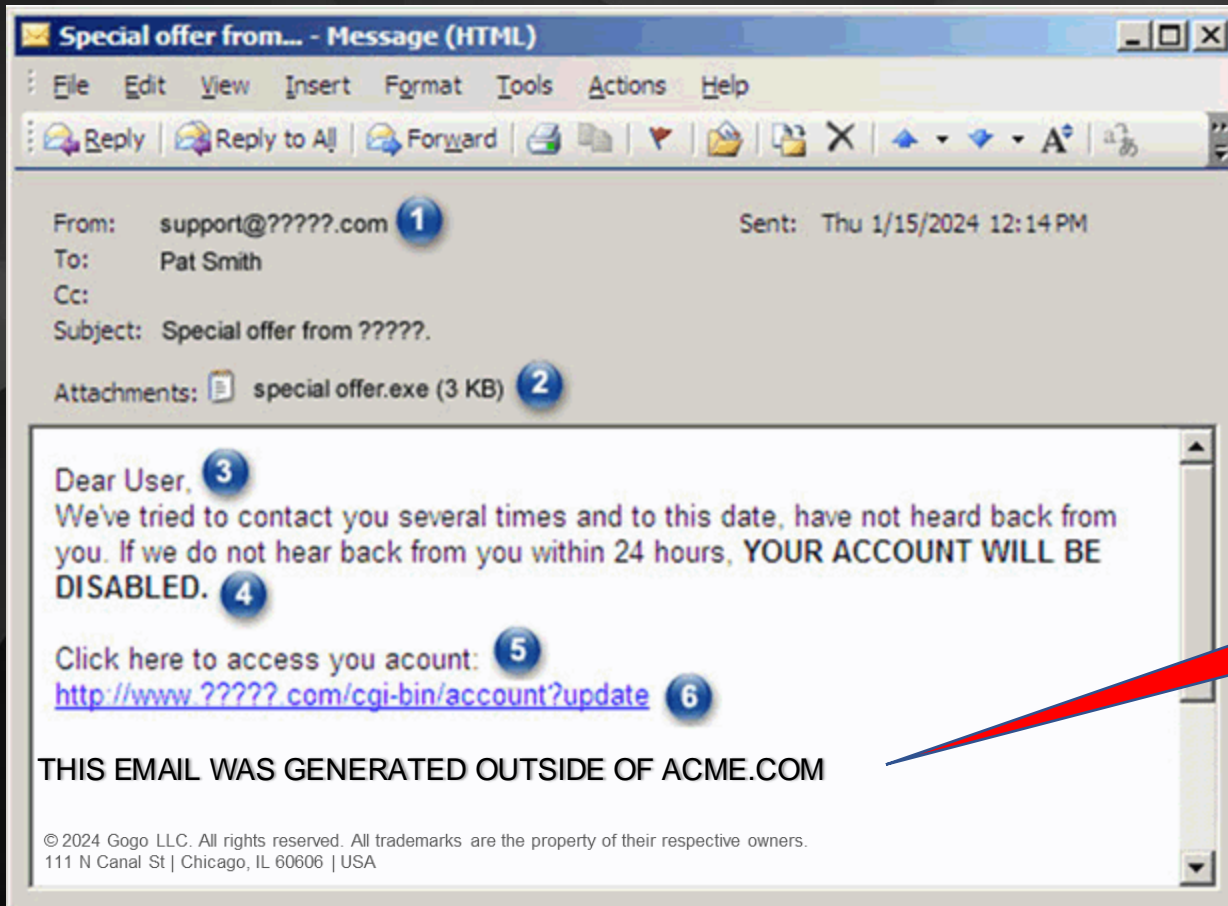
# SPEAR PHISHING ATTACK VECTOR



**DISTORTED OR INCORRECT LOGO**



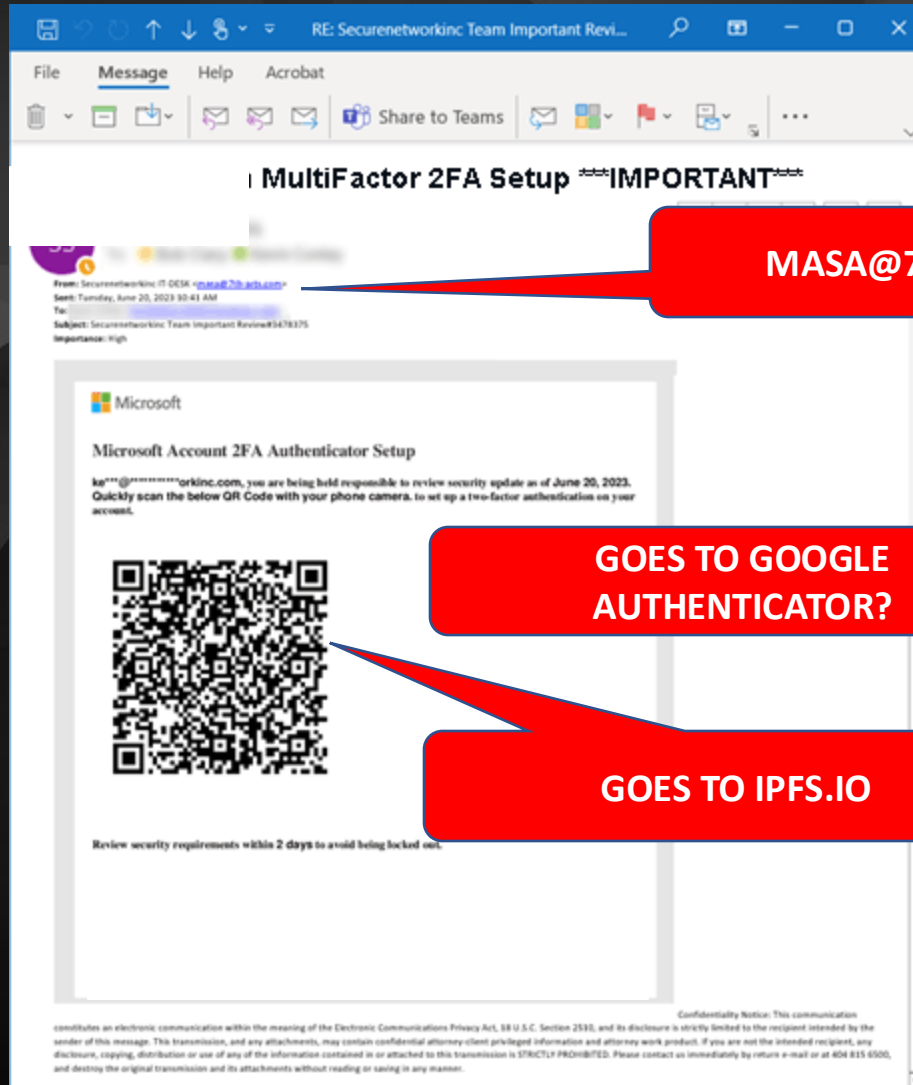
# SPEAR PHISHING ATTACK VECTOR



OUTSIDE GOGOAIR NETWORK

OUTSIDE NETWORK

# QR CODE PHISHING THREAT



MASA@7TH-ARTS.COM

GOES TO GOOGLE  
AUTHENTICATOR?

GOES TO IPFS.IO

STEALING CREDENTIALS

The screenshot shows a web form titled "Two-Factor Authentication Sign Up". It contains a QR code, a text input field for the verification code, and a dropdown menu for the two-factor code duration. A red callout box points to the QR code.

Two-Factor Authentication Sign Up

[QR Code]

Please scan this QR code with your Google Authenticator or TOTP app and then enter the verification code that appears.

Verification Code

Two-Factor Code Duration

Back Next

**SMS PHISHING = SMISHING**

**THE THREATS OF A  
NEFARIOUS TEXT MESSAGE**

# STOLEN DATA ON DARKWEB

Toolbox Cloud Browser

News-Canva-Dub x Problem loading x Problem loading x Problem loading x TorLinks | .onion x Dark Leak Market x

← → ↺ ⌂ <http://hvlccgrasynofno7tnyr6wofxd2rvpq5gebvu5m3cw7rjvndjmbgezid.onion/index4658.php?page=2> ☆ 📖

HOME GET HELP

## DARK LEAK MARKET

Leaked Database & Documents

OCTOBER, 2021 / PRICE: \$200

**DDC Data Leak**  
DNA Diagnostics Center (DDC), an Ohio-based DNA testing company, has disclosed 2,102,436 persons data.  
17678 VIEWS / 0 SOLD

OCTOBER, 2021 / PRICE: \$500

**Syniverse Data Leak**  
Syniverse is a major telecommunication company, almost all mobile carriers like AT&T and many more rely on its network.  
17991 VIEWS / 1 SOLD

OCTOBER, 2021 / PRICE: \$550

**Epik Domain registrar and web host**  
The breach includes a huge volume of data not just of Epik customers, but also WHOIS records belonging to individuals and organisations who were not Epik customers.  
17926 VIEWS / 1 SOLD

AUGUST, 2021 / PRICE: \$500

**Gigabyte Data Leak**  
Data of Gigabyte corp. internal company information from Gigabyte, along with private data about tech giants AMD and Intel  
27511 VIEWS / 4 SOLD

AUGUST, 2021 / PRICE: \$800

User Agent: TOR Browser Language: en-US,en Timezone: America/New\_York

## Fresh Leaks

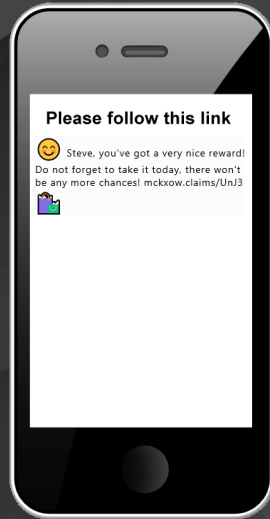
- ☐ Major indian cryptocurrency Data Leak
- ☐ US Cellular data leak Dec-2021
- ☐ T Mobile Data Leak Dec-2021

- ☐ UKG Kronos Data Leak
- ☐ Volvo data breach
- ☐ Panasonic data breach
- ☐ DDC Data Leak
- ☐ Syniverse Data Leak
- ☐ Epik Domain registrar and web host
- ☐ Gigabyte Data Leak

- ☐ AT&T Database Leak

- ☐ Pine Labs Data Leak
- ☐ DreamHost Data Leak
- ☐ Cognyte Data Leak

# SMISHING AKA: SMS PHISHING



**NEVER REPLY  
DELETE OR BLOCK CALLER**

# SMISHING AKA: SMS PHISHING



## NEVER CLICK ON THE LINK

# DARKWEB SMS PHISHING APPS

wallstyzjhkrvmj.onion/offer/4453



Search

Wall<sup>ST</sup> Market

[Home](#) [User-CP](#) [Support](#) [Messages](#) [Log Out](#)

Welcome, [potatoesalad](#)

Bank of America

## Info

Vendor: [eucarder](#) (2441) ★★★★★ (4.63)

Any questions about the offer?

☐ Digital goods  
☒ Multisig Escrow

bitcoin MONERO

★ Add to favorites

Amount

1

Buy

Scroll down for prices

## BANK OF AMERICA BUSSINES MOBILE EXPLOIT

Description

[Refund policy & Vendor information](#)

THIS METHOD WORKS ONLY WITH BUSINESS BANK ACCOUNTS, REGULAR ACCOUNTS WILL ONLY CLEAR AROUND \$2000

This method will help you to finish off and get the most out of your old or new bank drops, its best to avoid any type of ACH.

### Details

**Quantity in stock** 99 Piece

**Minimum amount per order:** 1 Piece

**Maximum amount per order:** 1 Piece

**Already sold:** < 10 Piece

**Category:** Software & Malware → Exploits

**Views:** > 2900

### Rating

Communication ★★★★★ (5)

Quality ★★★★★ (5)

### Prices


Amount	Price	Bitcoin	Monero
1	\$16.00/Piece	0.00403 BTC/Piece	0.30616 XMR/Piece



# SMISHING AKA: SMS PHISHING

① wallstyzjhrvmj.onion/offer/4453

Wall's Market Home User-CP Support Messages Log Out



**Info**  
Vendor: eucarder (2441) ★★★★★ (4.63)  
[Any questions about the offer?](#)  
☐ Digital goods  
☒ Multisig Escrow

## BANK OF AMERICA BUSSINES MOBILE EXPLOIT

Description Refund policy & Vendor information

THIS METHOD WORKS ONLY WITH BUSINESS BANK ACCOUNTS, REGULAR ACCOUNTS WILL ONLY CLEAR AROUND 10% OF THE BALANCE

This method will help you to finish off and get the most out of your old or new bank drops, its best to avoid any security issues

**Details**

**Quantity in stock** 99 Piece  
**Minimum amount per order:** 1 Piece  
**Maximum amount per order:** 1 Piece  
**Already sold:** < 10 Piece  
**Category:** Software & Malware → Exploits  
**Views:** > 2900


**Rating**

Communication  
Quality

**Prices**

Amount	Price	Bitcoin	Monero
1	\$16.00/Piece	0.00403 BTC/Piece	0.30616 XMR/Piece

9:50



**BANK OF AMERICA**

Username


Password

Login

Forgot Password?

Don't have an account? [Register Here](#)

9:50



**Bank of Moscow**

Username

Password

Login

Forgot Password?

Don't have an account? [Register Here](#)



**VOICE PHISHING = VISHING**

**THE THREATS OF A  
NEFARIOUS PHONE CALL**

# VOICE PHISHING OR VISHING

TELL ME ANYTHING



**JUST LISTEN, DONT ACKNOWLEDGE  
HAVE THEM PUT IT IN WRITING**

# VOICE PHISHING USING DARK AI

## Generate AI Voices

Try the live demo without signing in or sign in to synthesize text up to 5000 characters.

### Language



English (US)

### Voice



[Standard, Female] Salli



Text ( As a test purpose, only the first 300 characters will be synthesized )

Enter your text...

...d, up to 300 test characters.

### Audio controls

[sign up](#)

Speed

Tone

Volume

### Advanced effects

[sign up](#)

Angry

Cheerful

Excited

Newscast

Screaming

Whisper

Friendly

Hopeful

Sad

Terrified

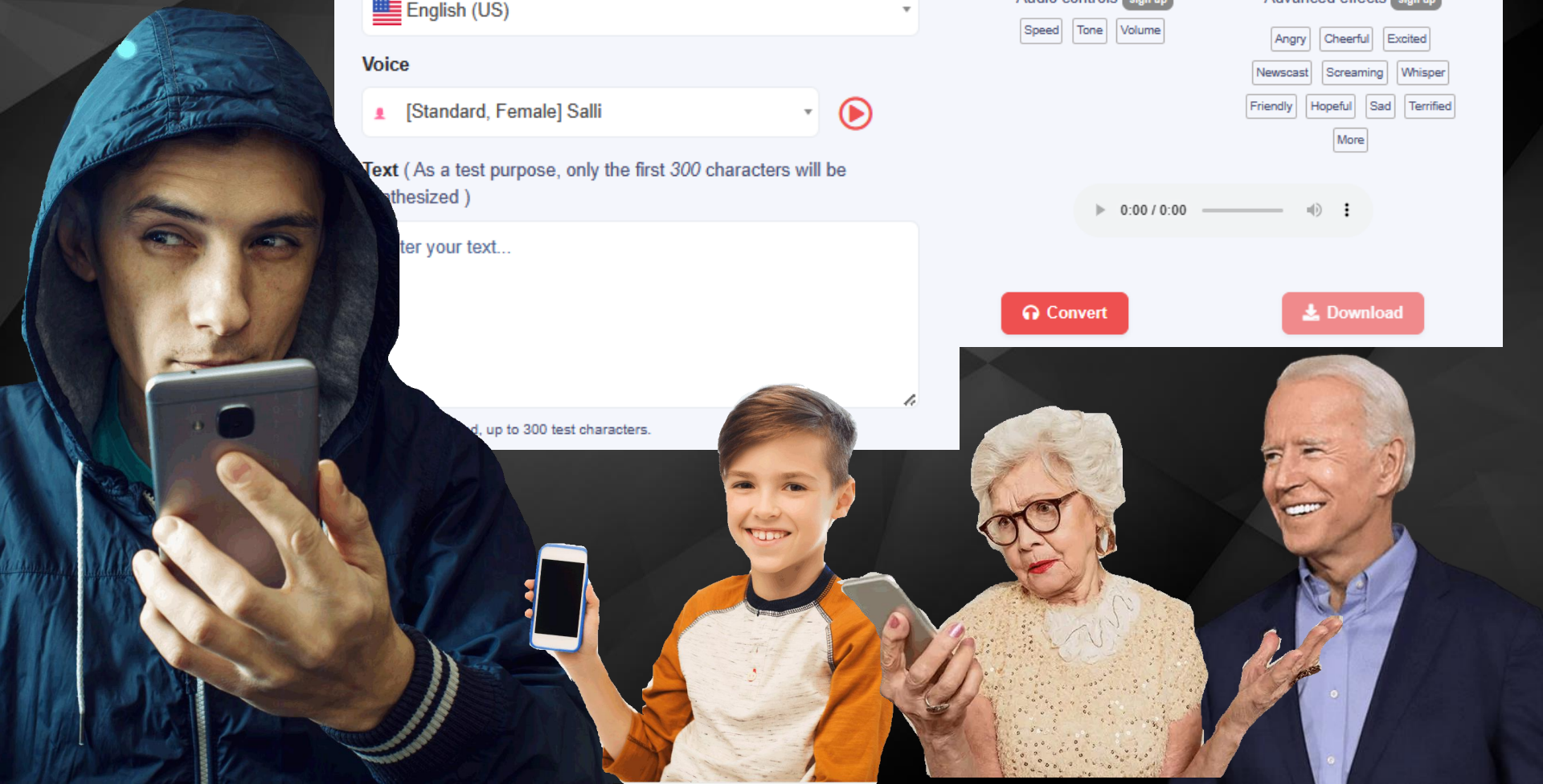
[More](#)

▶ 0:00 / 0:00



Convert

Download



# VOICE PHISHING OR VISHING

NEVER DISCUSS ANYTHING  
JUST HANG UP



WE NEVER CALL  
ANYBODY



# PROTECTING YOURSELF



**NEWS PROVIDES HACKING CONTENT**



**SOCIETAL VULNERABILITIES**

**PAY ATTENTION TO DETAILS**



**SLOW DOWN AND READ THE FINE  
PRINT**

**HOVER OVER THE LINKS**

**DO NOT REPLY TO UNKNOWN SMS  
TEXT MESSAGES**

**DO NOT TALK TO SCAMMER**



**EXAMINE EMAILS FOR  
QUESTIONABLE CHARACTERISTICS**

**EMAIL SCAMS ARE GETTING MORE  
SOPHISTICATED. EXAMINE CLOSELY**

**CONSIDER YOUR PHONE AN  
EXTENSION OF YOUR COMPUTER**



**ALWAYS CONTACT INFORMATION  
TECHNOLOGY IF YOU QUESTION  
SOMETHING**

# QUESTIONS?

Jim Ockenden  
Security Advisor  
315.949.2803 | Office  
315.374.6721 | Mobile  
[jim@securenetworkinc.com](mailto:jim@securenetworkinc.com)