

October Is Cybersecurity Awareness Month

Staying 24/7 Cyber Safe In A Modern World



Jessica Blushi
Keenan &
Associates



Tim Femister
Firestorm Global



Erik Ramirez
Cybersecurity and
Infrastructure Security
Agency (CISA)

October 1st, 2024

Background



Erik Ramirez

Cybersecurity and Infrastructure
Security Agency (CISA)

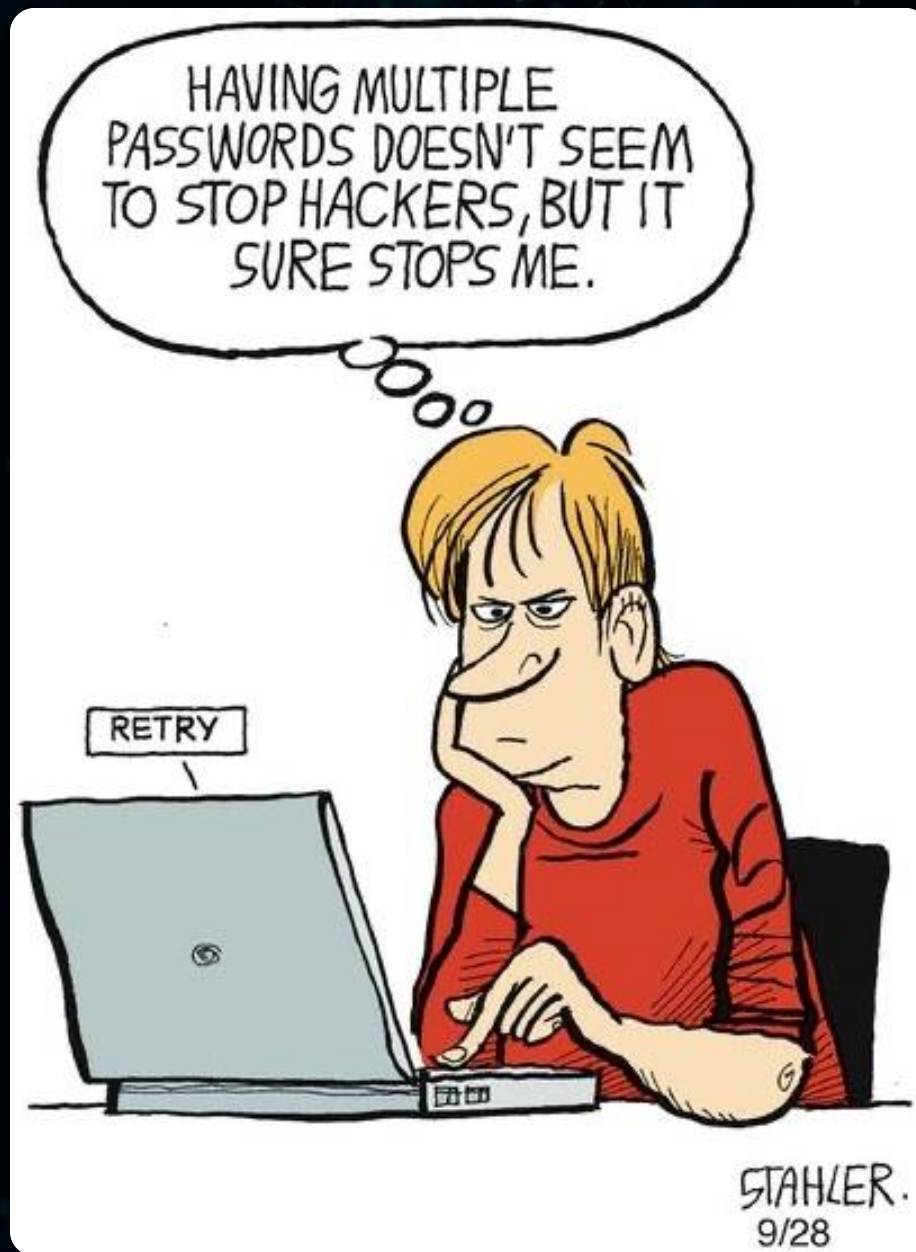
- Dedicated Cybersecurity Training & Exercise Specialist
- Partners with Technical and Non-Technical Audiences
- 5-Years in large K-12 education
- Master's in Organizational Leadership



Tim Femister

Firestorm Global

- Founder and Principal at Firestorm Global
- Supports 400+ K-12 schools and colleges across California
- 15+ Years experience working with K-12, Higher Ed and Municipalities
- Media contributions to Forbes, NBC, Lifetime and more



Cybersecurity In 2024

Home > News > Security

'Fortune 50' Company Made Record-Breaking \$75M Ransomware Payment

The payment was sent to a lesser known ransomware group called Dark Angels, according to cybersecurity vendor Zscaler, topping the \$40 million paid by CNA in 2021.

By [Michael Kan](#)

July 30, 2024



Hackers email stolen student data to parents of Nevada school district

By [Lawrence Abrams](#)

October 28, 2023 02:11 PM 0



[Schools](#)

Hackers Steal \$6M Meant For School Bus Contract

"It is unbelievably unethical that someone would steal this amount of money from taxpayers, from children," Mayor Justin Elicker said.



New Haven Independent, News Partner

Posted Thu, Aug 10, 2023 at 4:48 pm ET



Finance worker pays out \$25 million after video call with deepfake 'chief financial officer'

By Heather Chen and [Kathleen Magramo](#), CNN

2 minute read · Published 2:31 AM EST, Sun February 4, 2024



- **Mega ransom payments** and financial impact
- **Public Education increasingly targeted** (with and without malware)
- Hackers are **stealing student data** and **extorting parents**
- **Deepfake scams** are rapidly evolving and causing havoc

***Confirmed* Ransom Payments Exceed \$1B For First Time.**

 **NBC NEWS**

WATCH LIVE



SECURITY

Ransomware hackers raked in a record \$1 billion from victims last year

Despite efforts to contain the ransomware criminal ecosystem, the promise of wealth and the relative lack of consequences have spurred more ransomware hackers than ever before.



How Does This Happen? 🤖

How Does This Happen?



You Give It To Them



**Something You Trust
Gives It To Them**

How Does This Happen?



You Give It To Them



**Something You Trust
Gives It To Them**

How Does This Happen?

Human Error Contributed To 68% Of Data Breaches Last Year

Why Does This Happen So Often?



**Anyone Can Email, Call,
or Text You Right Now.**

Literally.

Traditional Communication Channels Were Originally Built On Trust

Website statistics: 2474 active paid members and over than 3647546 emails sent since 2008.

Send Fake Anonymous Email

Your message below will contain advertising text, warning message and IP address of you.

For a real prank email you need to be a paid member.

From Name : (Optional)

From E-mail : *

To : *

Subject : *

Continue

1. Click on "Continue"
2. Activate your account
3. Access your content



storagecfd.com

Rich text editor toolbar with icons for Bold, Italic, Underline, Text Color, Background Color, Bulleted List, Numbered List, Indent, Outdent, Link, Unlink, Image, Smiley, Media, and HTML. Below the toolbar are dropdown menus for Paragraph, Font family, and Font size, followed by a table icon and zoom in/out buttons.

Hi Colleen,

I spoke with Jeremy at XYZ Transit and confirmed their new banking information at Example Bank. Please see the details below. We're past due, so let's process today to avoid service disruption.

John

Cyber Criminals Know How To Send Fake, Targeted Emails.

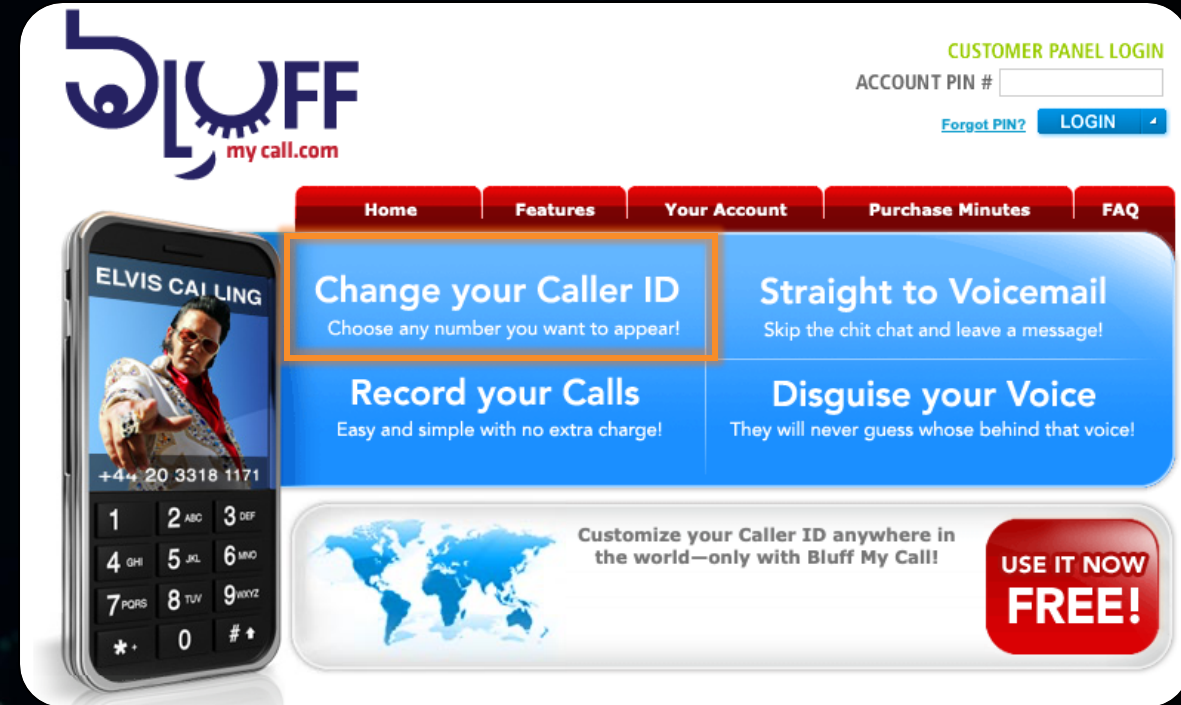
Phishing: Fraudulent Email

Spear Phishing: Targeted Fraudulent Email

Cyber Criminals Can Easily Spoof (Fake) A Phone Number In Minutes.

Vishing: Fraudulent Phone Call

Smishing: Fraudulent Text Message



Cyber Criminals Are Rapidly Pursuing Voice Cloning (Deepfakes)

Deepfake: Digitally Altered Voice Or Video

AI Voice Cloning: Clone your Voice in Seconds

Over 1,000,000 users create high quality replicas of their voice by deploying the most cutting-edge AI voice cloning model. Use your own voice data to gain unparalleled control over synthetic speech and capture human emotion in stunning detail.

Clone your voice for free



Beth

Real Voice



Cloned Voice



Seth

Real Voice





Cloned Voice



Cyber Criminals Are Rapidly Pursuing Voice Cloning (Deepfakes)



Deepfake: Digitally Altered Voice Or Video

**CorentinJ/Real-Time-Voice-Cloning**  Star

Clone a voice in 5 seconds to generate arbitrary speech in real-time



[python](#) [deep-learning](#) [tensorflow](#) [pytorch](#) [tts](#)

● Python · ☆ 48k · Updated 18 hours ago

**KevinWang676/Bark-Voice-Cloning**  Star

Bark Voice Cloning and Voice Cloning for Chinese Speech

● Jupyter Notebook · ☆ 826 · Updated 7 days ago

**PlayVoice/whisper-vits-svc**  Star

Core Engine of Singing Voice Conversion & Singing Voice Clone



Posts: 969
Threads: 20
B Rating: 14 ⬆️ 0
Popularity: 933
Bytes: 🟢 6,480.19
Game XP: 3,115

Introducing my newst creation, "WormGPT." This project aims to provide an alternative to ChatGPT, one that lets you do all sorts of illegal stuff and easily sell it online in the future. Everything blackhat related that you can think of can be done with WormGPT, allowing anyone access to malicious activity without ever leaving the comfort of their home. WormGPT also offers anonymity, meaning that anyone can carry out illegal activities without being traced.

Features:

- Fast and stable replies
- Unlimited characters
- Privacy focused
- Blackhat allowed
- Save results in txt file
- Different AI models

Planned features:

- System role - in order to get more accurate results you can set a role to the AI (example: senior developer in c#)
- Hosted website - everything hosted online, no downloads, no executables

Preview

```
C:\Users\rui\OneDrive\Desktop\WormGPT X + -
WORMGPT
Welcome to the WormGPT. The biggest enemy of the well-known ChatGPT!
LAST\rui\rui Write me a python malware that grabs computer's username, external ip address, and google chrome cookies, zip everything and send to a discord webhook
20:24:28 PM
```

Dark AI Is Breaking Down Language Barriers And Accelerating Attacks

Putting It All Together



Wire Instructions For Emergency Support Services



○ Todd Jacobs <tjacobs@criticalservices.org>

To: ● Kathy Faye Cc: John Hanley <jhanley@yourdist...>

Hi Kathy,

Superintendent Hanley asked me to send you my wire information for emergency support services. Once payment is received, we will start our process immediately. Thank you for your prompt support as this remains extremely time sensitive.

Wire Information:

- Superintendent's cell phone number is spoofed by a bad actor
- Deepfake audio mimics a familiar voice utilizing prior Board meeting recording
- Email appears legitimate at first glance and instructions align to the phone call received

Rely On Strong Fundamentals

Check The Sender Address

Rely On Strong Fundamentals



or



FW: Districtwide Safety Protocols




○ Susan Johnson <susan.johnson@yourdistrict.org>

To: ● Josh Garrison

Rely On Strong Fundamentals

FW: Districtwide Safety Protocols



 Susan Johnson <susan.johnson@yourdistrict.org>

To: Josh Garrison



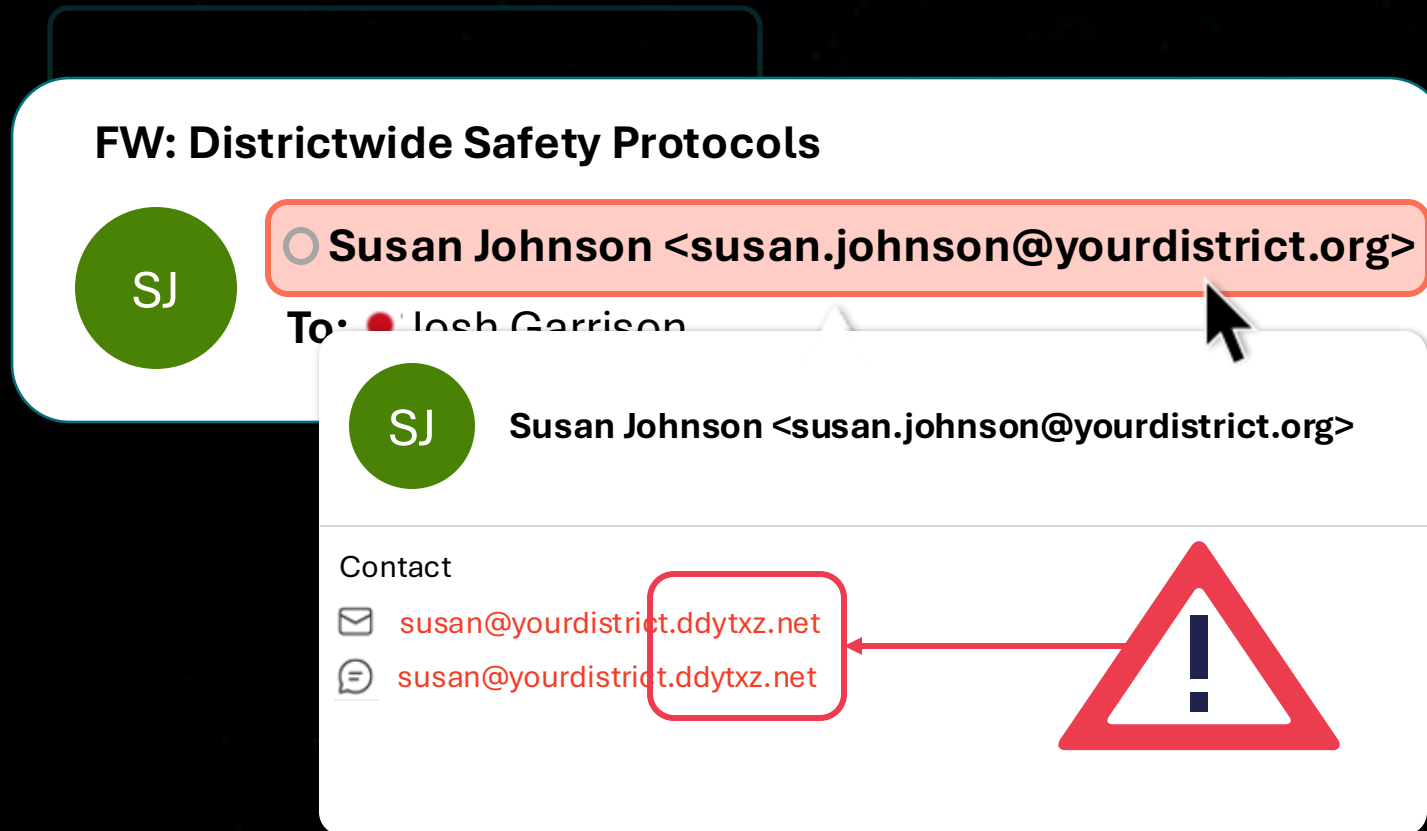
Susan Johnson <susan.johnson@yourdistrict.org>

Contact

 susan@yourdistrict.ddytzx.net

 [susan@yourdistrict.ddytzx.net](tel:susan@yourdistrict.ddytzx.net)

Rely On Strong Fundamentals



- Click on the Sender to identify the true email address
- Report as phishing and delete if you don't recognize the domain name
- The domain is the very last part of the address, such as ddytxz.net or google.com (not 'yourdistrict')

Rely On Strong Fundamentals

Check The Sender Address

**Don't Click Links Or
Attachments From
Unknown Senders**

Rely On Strong Fundamentals

Hi Debbie,

Chris has listed you as a reference for a position he has applied at our district.

If you're willing to provide a reference, please click the below link:

<http://www.checkr.bckrnd.ru/>

www.checkr.com/position-reference

Note: If you did not agree to be a reference, you may [unsubscribe](#) by [clicking here](#).

Thank you,

Jean

Rely On Strong Fundamentals

Hi Debbie,

Chris has listed you as a reference for a position he has applied at our district.

If you're willing to provide a reference, please click the below link:

www.checkr.com/position-reference

<http://www.checkr.bckrnd.ru/unsubscribe>

Note: If you did not agree to be a reference, you may [unsubscribe](#) by [clicking here](#).

Thank you,

Jean

Rely On Strong Fundamentals

Check The Sender Address

**Don't Click Links Or
Attachments From
Unknown Senders**

**Evaluate Tone, Grammar
And Syntax**

Email not displaying correctly? [View it](#) in your browser



Dear Customer,

We're letting you know that we've detected some unusual activity on your card on 12/28/2019. For your security, please verify the following transaction(s) so that you can continue to use your card

Do you recognize all of these transaction(s)?

Approved transaction at SQC*CASH APP for \$224.49 on 12/28/2019

Declined transaction at TOP UP B.V. for \$624.11 on 12/28/2019

Approved transaction at BESTBUY for \$124.59 on 12/28/2019

YES, I recognize all of these transactions

YES will make your card immediately ready to use again

NO, I don't recognize one or more of these transactions

NO will allow you to complete the verification process and file a fraud claim in Online or Mobile Banking

Rely On Strong Fundamentals

Check The Sender Address

**Don't Click Links Or
Attachments From
Unknown Senders**

**Evaluate Tone, Grammar
And Syntax**

**Place An Outbound Call To
A Trusted Number**

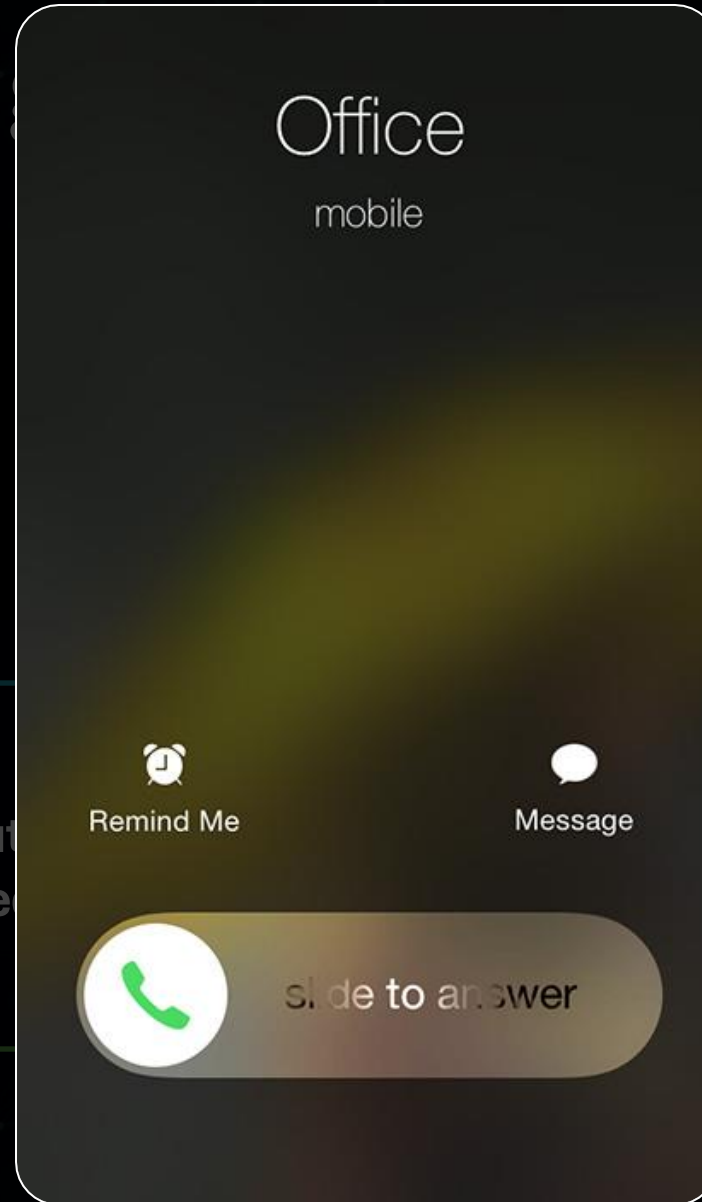
Rely On Strong

als

Check The Sender Address

Evaluate Tone, Grammar
And Syntax

Place An Out
A Truste



Rely On Strong Fundamentals

Check The Sender Address

**Don't Click Links Or
Attachments From
Unknown Senders**

**Evaluate Tone, Grammar
And Syntax**

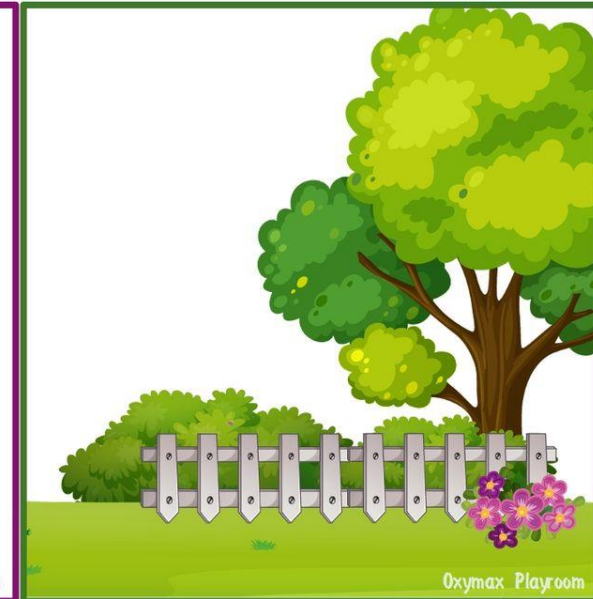
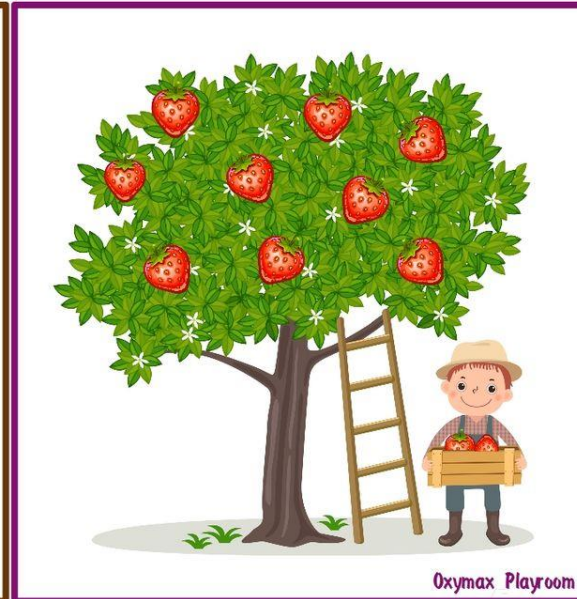
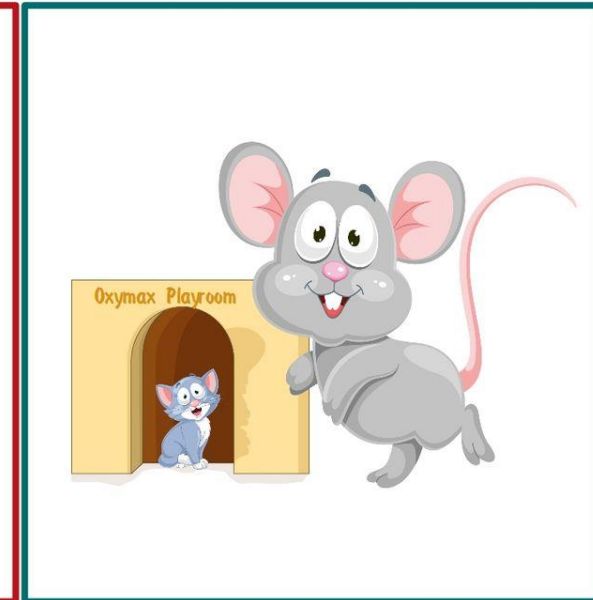
**Place An Outbound Call To
A Trusted Number**

**Watch And Listen For Out
Of Place Occurrences**

Re

Chec

mmar



Rely On Strong Fundamentals

Check The Sender Address

**Don't Click Links Or
Attachments From
Unknown Senders**

**Evaluate Tone, Grammar
And Syntax**

**Place An Outbound Call To
A Trusted Number**

**Watch And Listen For Out
Of Place Occurrences**

Remember: When In Doubt, Ask For A Second Set of Eyes 🧐

24/7 Cyber Safe Best Practices

- 1 Report, But Do Not Forward Phishing Messages
- 2 Never Send Money Without Verification (Call Trusted Numbers)
- 3 Use Strong, Unique Passwords (👍 Password Managers)
- 4 Keep Software Updated (Especially Security Updates 🚨)
- 5 Utilize Multifactor Authentication Wherever Possible

SAFER Cyber Risk Assessment

- **Complimentary Cybersecurity Assessment**
- Structured risk assessment **aligned to NIST**
- Standard engagement covers 100+ topics
 - **2.5-hour engagement** followed by **1-hour readout**
 - ~40 slide engagement report with clear, concise recommendations
- Initiate engagement at www.firestormglobal.com/safer
- **Questions?** Email SAFER@firestormglobal.com

Engagement Domains Snapshot

The Engagement Domains Snapshot serves to provide an overall rating for the current state maturity of the cybersecurity environment as reviewed through the engagement.

OVERALL MATURITY
Proactive



	CORRECT DOMAINS	LOW MATURITY	HIGH MATURITY
Strategy	1 2 3 4 5	1 2 3 4 5	1 2 3 4 5
Protect	1 2 3 4 5	1 2 3 4 5	1 2 3 4 5
Detect	1 2 3 4 5	1 2 3 4 5	1 2 3 4 5
Correct	1 2 3 4 5	1 2 3 4 5	1 2 3 4 5
Govern	1 2 3 4 5	1 2 3 4 5	1 2 3 4 5

Copyright 2024. Confidential Material. All Rights Reserved.

Engagement provided by Keenan as a service to its members.

Protect

Security Training and Awareness

Priority
1 2 3 4 5
Current State
<ul style="list-style-type: none"> Security awareness program has not been implemented Currently not performing awareness trainings, simulated phishing or similar awareness activities
Associated Risk
Lack of security awareness can lead to users accidentally clicking or downloading malicious content resulting in a significant event, such as a widespread ransomware incident

Maturity
1 2 3 4 5
Target Maturity
<ul style="list-style-type: none"> Regularly conducts security awareness training for all users Conducts appropriate phishing simulations for staff Enables users to report phishing attempts Communicates frequently to users about current cybersecurity events for deeper awareness Consider leveraging Human Firewall posters or similar items to support awareness
Recommended Remediation
Implement a recurring cyber awareness program incorporating appropriate training and simulated phishing
Framework Alignment
NIST 800-53 AT-2, AT-3

Copyright 2024. Confidential Material. All Rights Reserved.

Engagement provided by SAFER as a service to its members.

Q&A





Thank You

**FIRESTORM
GLOBAL**

firestormglobal.com