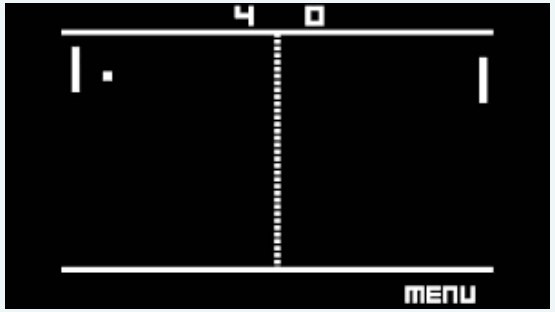
CYBER SECURITY DEEP DIVE

Presented by Paul Jones
CIO, City of West Palm Beach
CISSP, CISA, Security+, GLEG, ITIL Expert, Project+

#FGFOA2023

Remember When!!

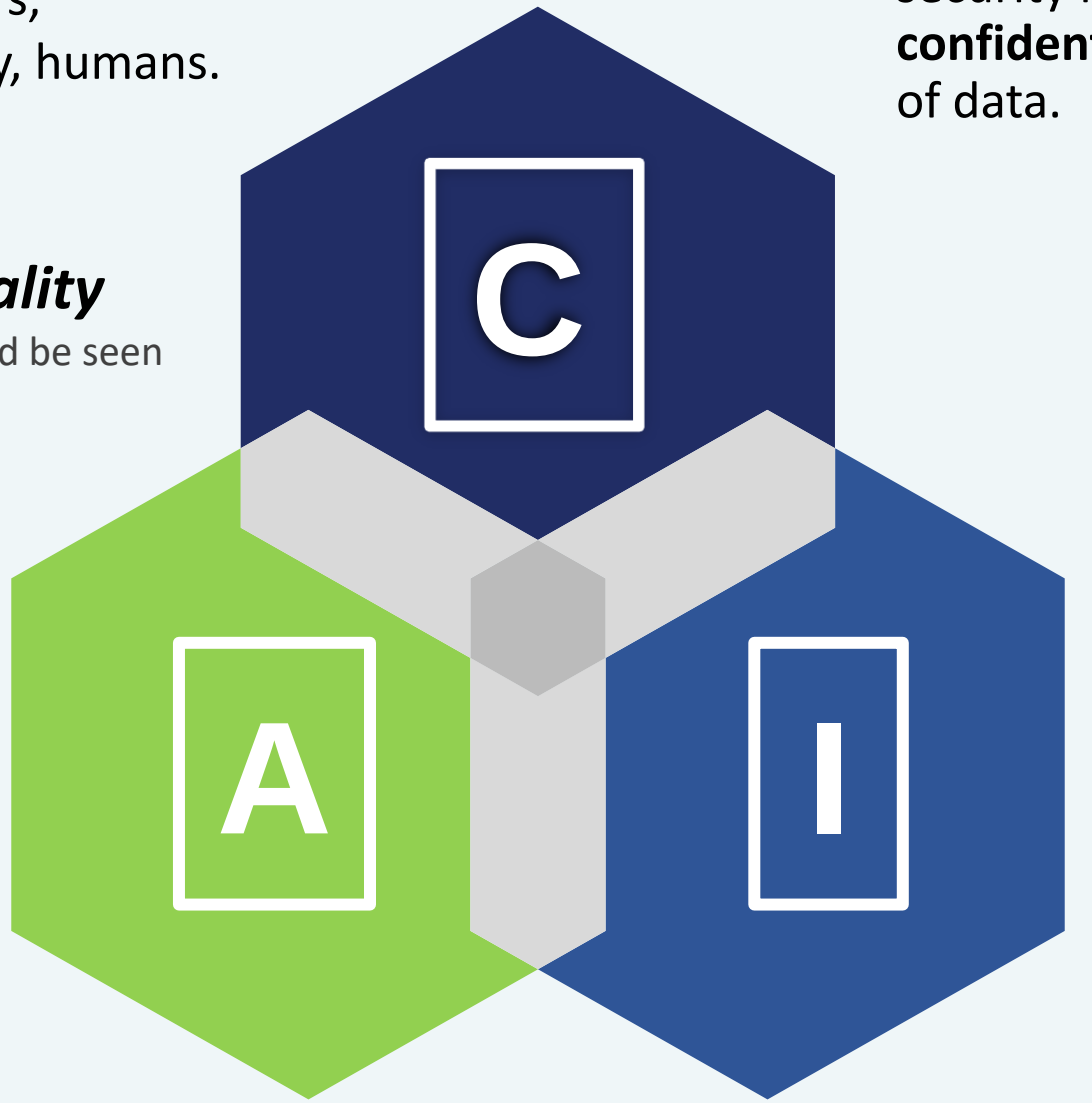


#FGFOA2023

Cyber Security

Cyber Security - assures asset protection, including data, desktops, servers, buildings, and most importantly, humans.

Cyber Security - the process of applying security measures to ensure **confidentiality, integrity, and availability** of data.



Confidentiality

Only see what should be seen

Availability

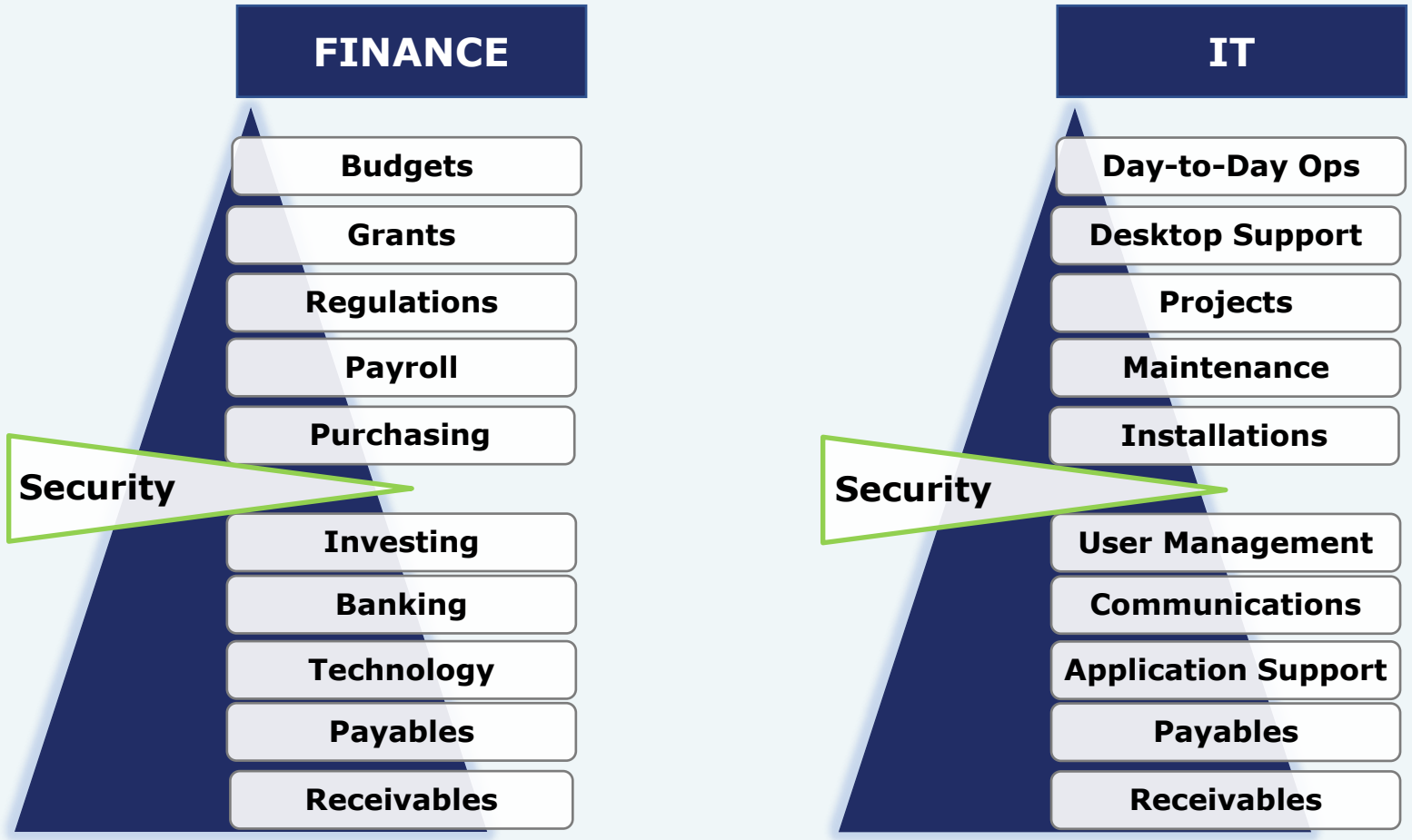
Can I get what I need when I need it

Integrity

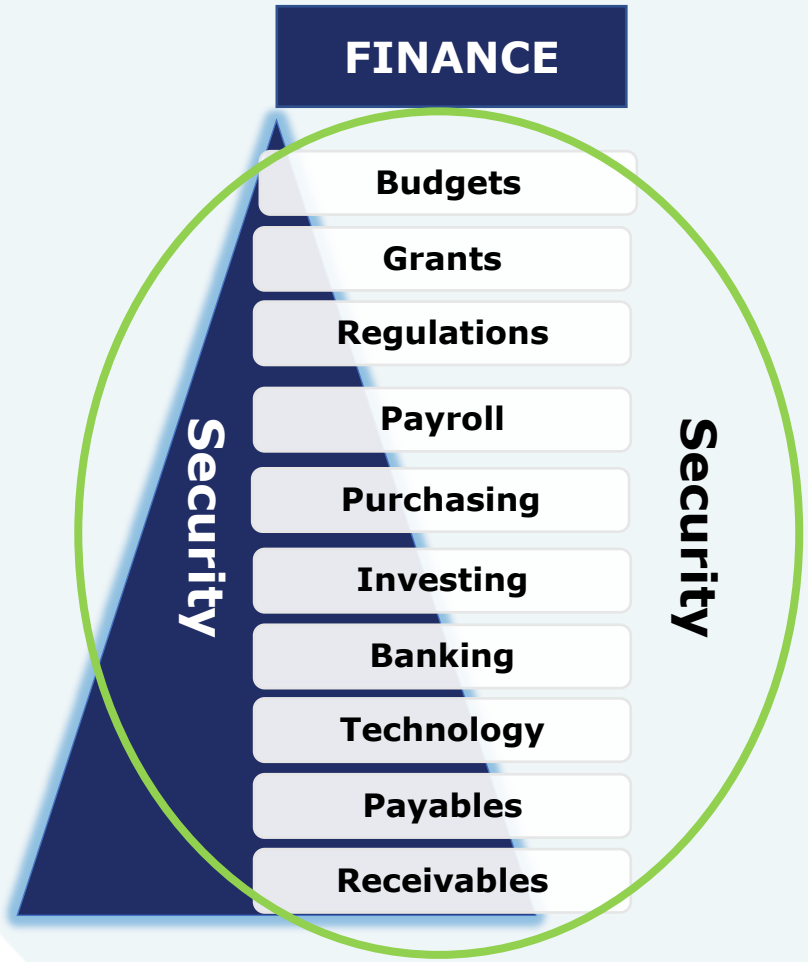
Accuracy of data.

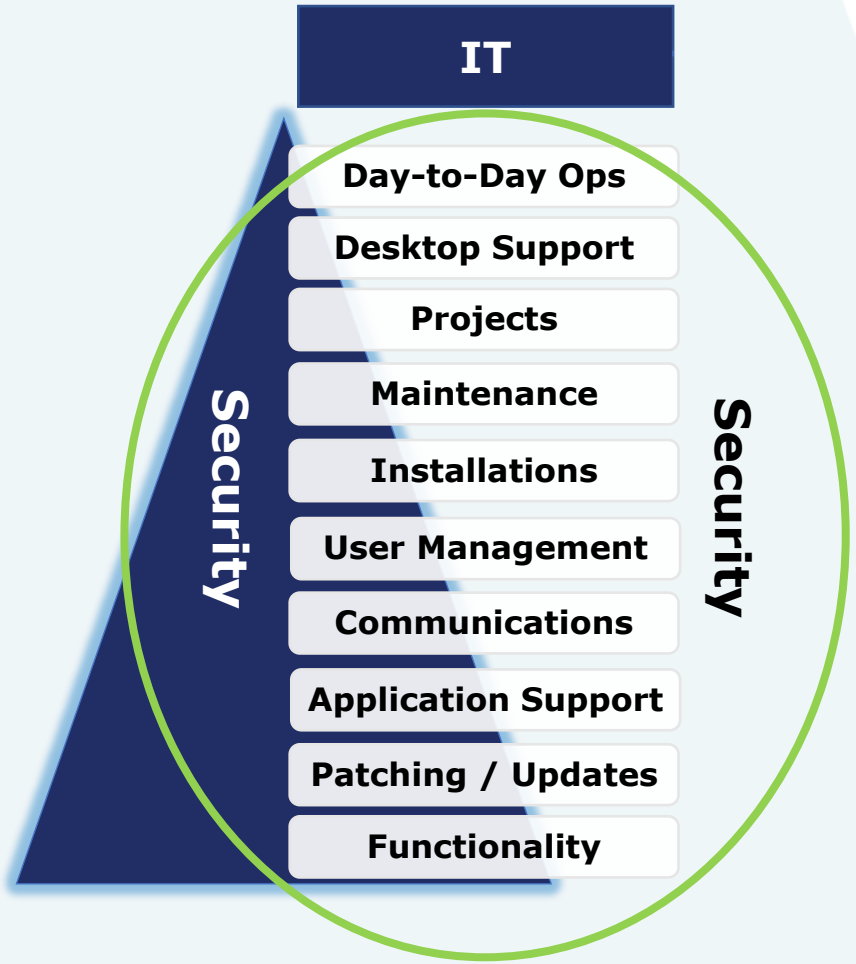
#FGFOA2023

The Challenge



The Goal


FINANCE
Budgets
Grants
Regulations
Payroll
Purchasing
Investing
Banking
Technology
Payables
Receivables
Security
Security


IT
Day-to-Day Ops
Desktop Support
Projects
Maintenance
Installations
User Management
Communications
Application Support
Patching / Updates
Functionality
Security
Security

Online Dangers

- There is a hacker attack every 39 seconds
- 300,000 new pieces of malware are created every day
- 92% of malware that businesses encounter is delivered via email
- Most breaches involve phishing and using stolen credentials
- Today's cybercriminals are motivated by the illicit profits of online crime
- More than 6,000 criminal marketplaces sell ransomware products and services
- Cybercrime is more profitable than the global illegal drug trade
- Hackers have exposed the personal information of 110 million Americans
- 27% of data breaches involved internal actors
- Costs of cybercrime are estimated to reach $10 trillion by 2025

Question - 1

The CIA Triad Includes:

A Confidentiality, Integrations, Access

B Concealment, Integrity, Accessibility

C Confidentiality, Integrity, Availability

D Conformity, Interfaces, Availability

Question - 1

The CIA Triad Includes:

A Confidentiality, Integrations, Access

B Concealment, Integrity, Accessibility

C Confidentiality, Integrity, Availability

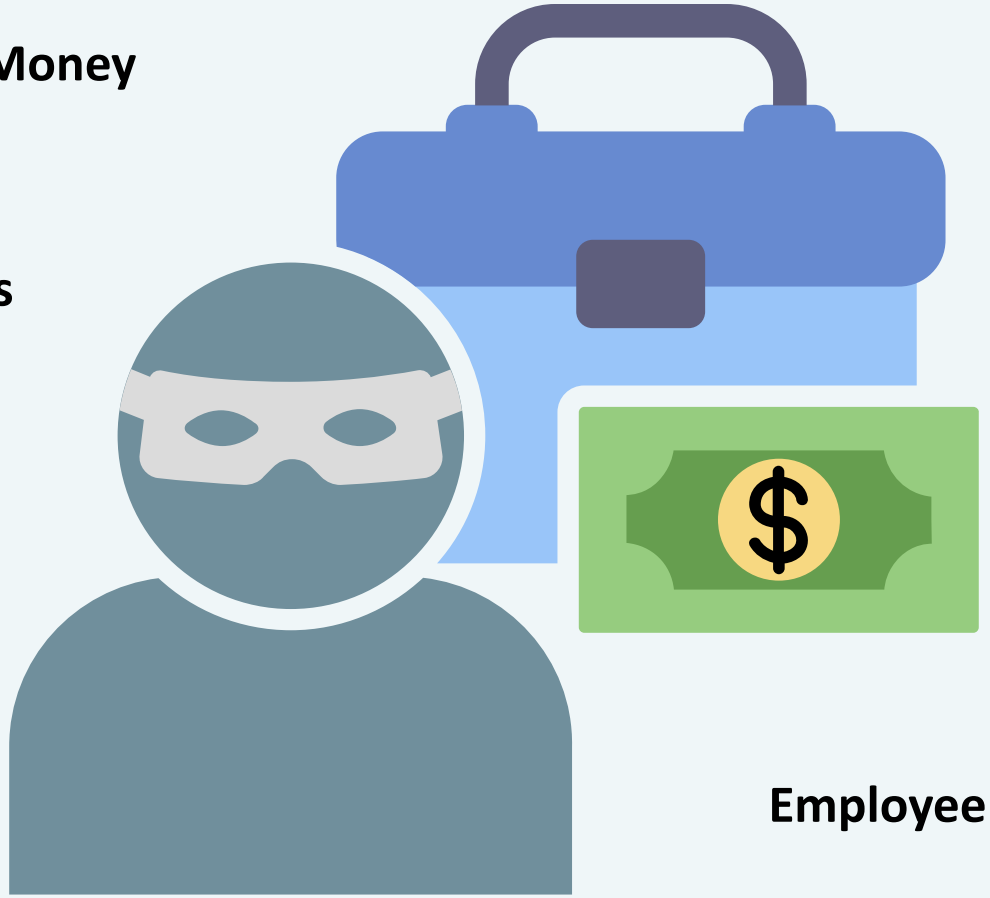
D Conformity, Interfaces, Availability

Finance a Bad Actor's Dream

Personally Identifiable Information (PII)

Credit Cards

Money, Money, Money



Wire/ACH Transactions

Social Security Numbers

Payroll Information

Banking Information

Direct Payments

Direct Deposits

Employee Information

Automatic Draws

Vendor Information

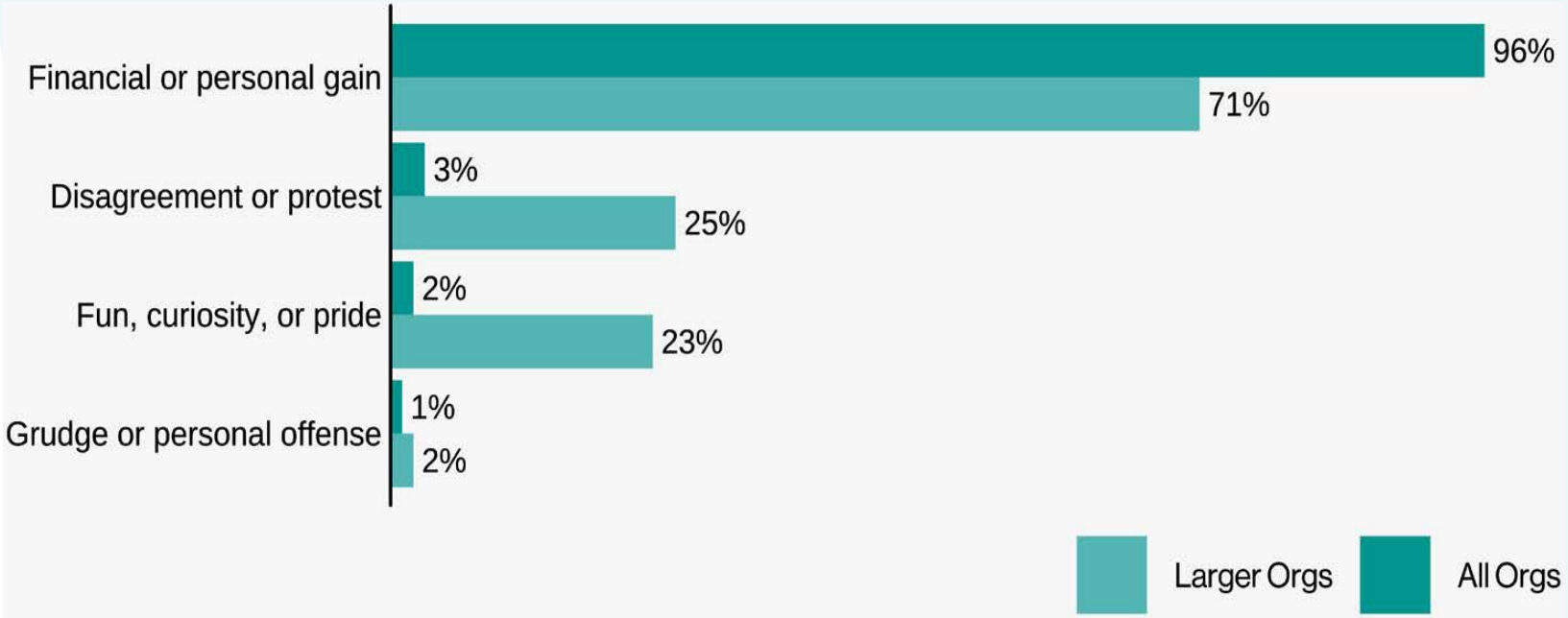
#FGFOA2023

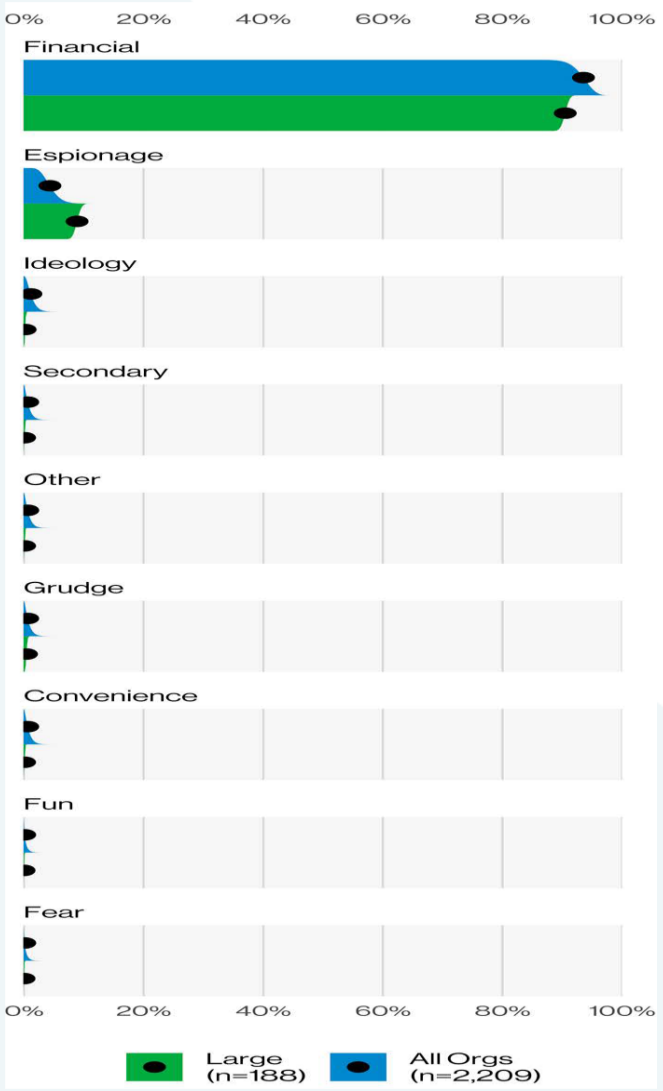
The Target

The Financial Sector continues to be victimized by financially motivated organized crime, often via actions of Social (Phishing), Hacking (Use of stolen credentials) and Malware (Ransomware). Finally, Miscellaneous Errors, often in the form of Mis-delivery, is still very common.

Verizon Data Breach Investigations Report for 2022

Why Would Anyone Do This





Verizon Data Breach Investigations Report for 2022

MONEY, MONEY, MONEY

#FGFOA2023

The Culprit

Organized Crime = 79%

Verizon Data Breach Investigations Report for 2022

Key Threats!!

Basic Web Application Attacks These attacks are against a Web application, and after initial compromise, they do not have a large number of additional Actions.

System Intrusion Complex attacks that leverage malware and/or hacking to achieve their objectives.

Miscellaneous Errors Incidents where unintentional actions directly compromise secure information.

Social Engineering A psychological compromise of a person that alters their behavior into taking an action or breaching confidentiality.

Privilege Misuse Incidents driven by unapproved or malicious use of legitimate privileges.

Denial of Service Attacks Compromise the availability of networks and systems.

Lost and Stolen Assets Incidents where an information asset went missing, whether through misplacement or malice.

Everything Else This “pattern” isn’t a pattern at all. Instead, it covers all incidents that don’t fit within the orderly confines of the other patterns.

Verizon Data Breach Investigations Report for 2022

Key Finance Threats!!

Basic Web Application Attacks - These attacks are against a Web application, and after initial compromise, they do not have a large number of additional Actions.

System Intrusion - Complex attacks that leverage malware and/or hacking to achieve their objectives.

Miscellaneous Errors - Incidents where unintentional actions directly compromise secure information.

Social Engineering - A psychological compromise of a person that alters their behavior into taking an action or breaching confidentiality.

Verizon Data Breach Investigations Report for 2022

2nd Question?

According to the 2022 Verizon Breach Investigation Report, which is not one of the top key finance threat vectors?

- **A** Loss or stolen assets
- **B** Miscellaneous Errors
- **C** System Intrusion
- **D** Social Engineering

2nd Question?

According to the 2022 Verizon Breach Investigation Report, which is not one of the top key finance threat vectors?

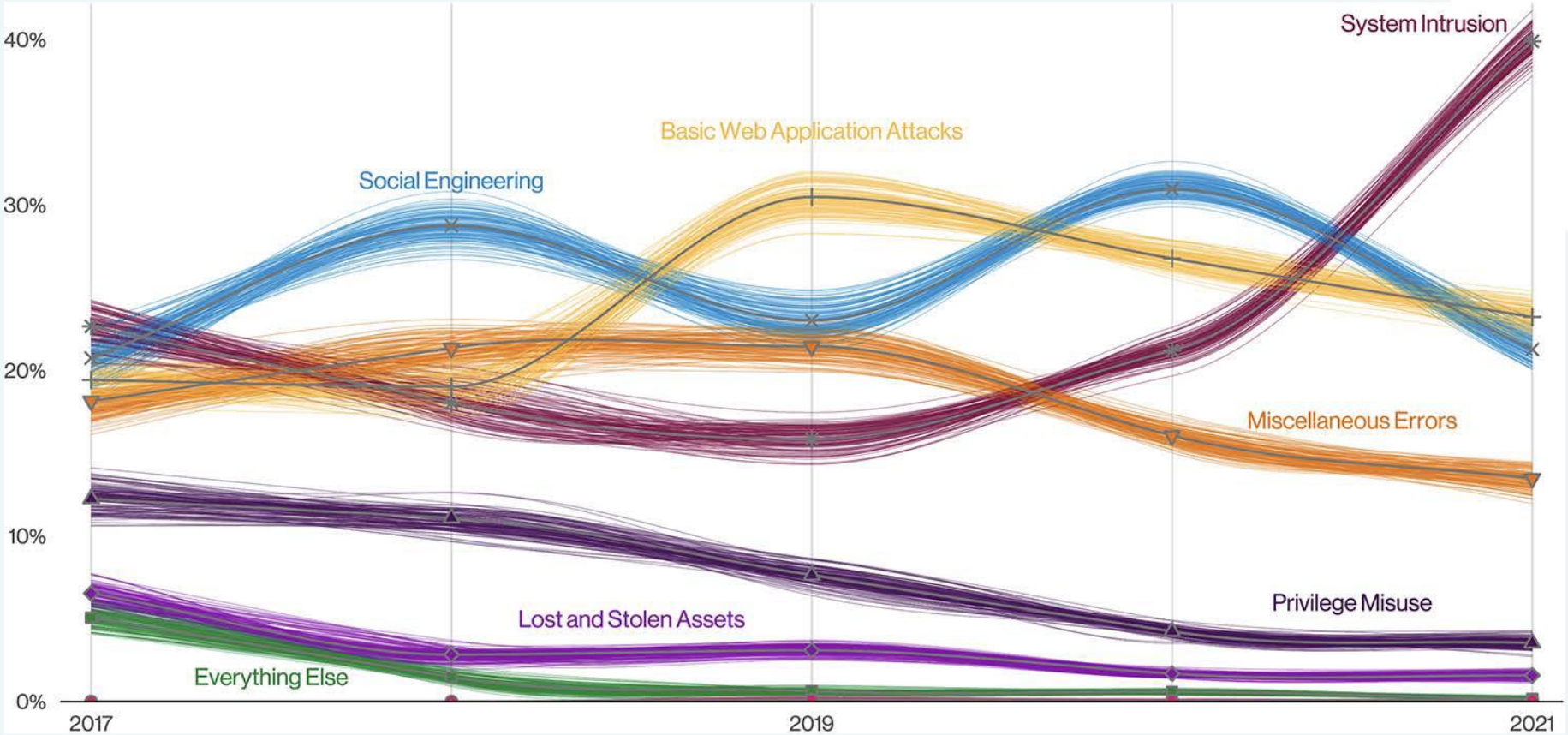
A. Loss or stolen assets

B. Miscellaneous Errors

C. System Intrusion

D. Social Engineering

The Numbers



Verizon Data Breach Investigations Report for 2022

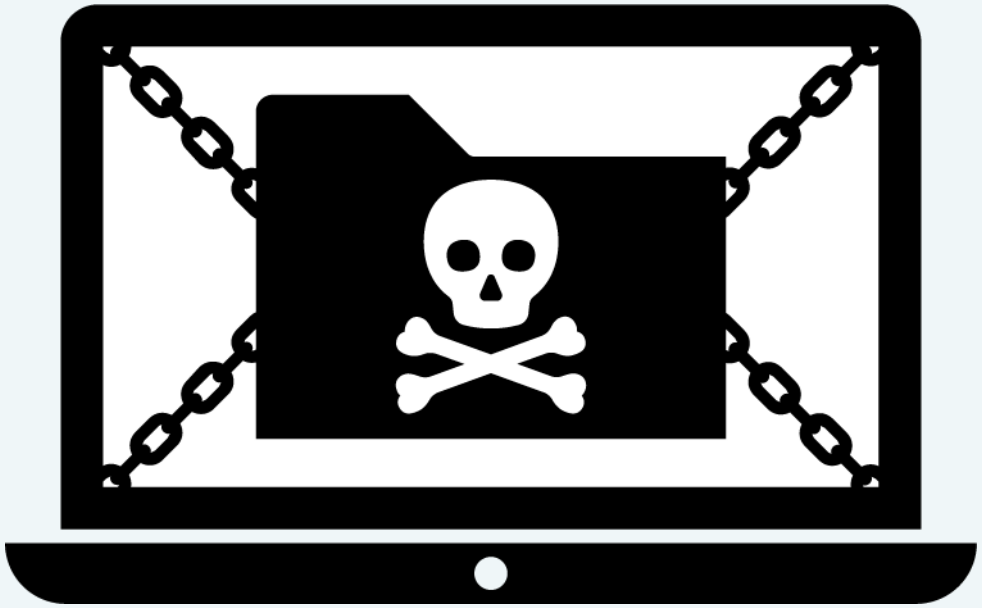
Breach Statistics

According to **The Identity Theft Research Center (ITRC) Annual Data Breach Report,** 2022 had the second-highest number of data compromises in the U.S. in a single year. At least 422 million individuals were impacted.

According to the FBI's **Internet Crime Report 2022**, 800,944 complaints of cybercrime were reported to the FBI by the public, a 5 percent decrease from 2021. However, the potential total loss increased to $10.2 billion in 2022, up from $6.9 billion in 2021. California, Florida, and Texas had the highest number of cybercrime victims.

Let’s Talk Ransomware

$456.8 million extorted in 2022



There are four main categories of ransomware:

1. **Encryption** - Encrypts data and makes it impossible to unlock without a decryption key.
2. **Lockers** - Restricts the use of your computer, making it impossible to work or use basic functions until the ransom is paid.
3. **Scareware** - Attempts to scare users into buying unnecessary software.
4. **Doxware/Leakware** - Threatens to leak personal or company data unless the ransom is paid.

Basic Protection

- Backup Data and Verify Restores
- Keep Backups Isolated
- Keep All Systems and Software Updated
- Install Antivirus Software and Firewalls
- Network Segmentation
- Email Protection
- Application Whitelisting
- Endpoint Security
- Limit User Access Privileges
- Run Regular Security Testing
- Security Awareness Training

No More Payout

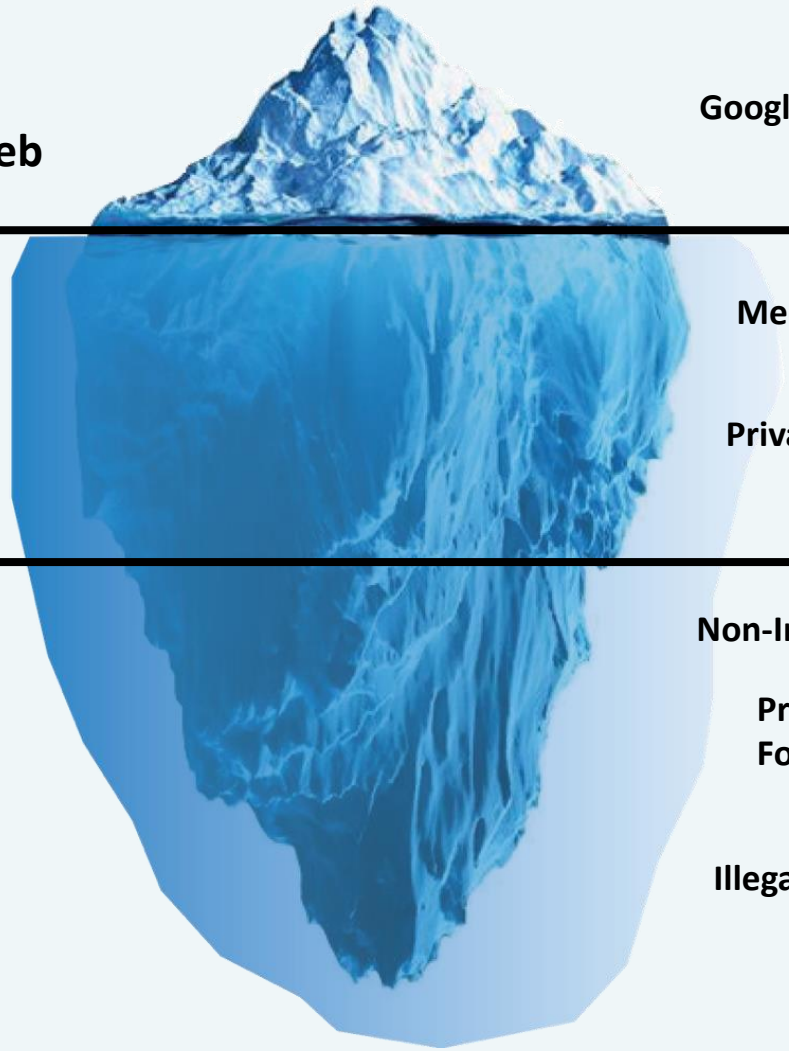
Florida amended its State Cybersecurity Act to prohibit state agencies, counties, and municipalities experiencing a ransomware attack from paying or otherwise complying with a ransom demand.

#FGFOA2023

The Market Place

#FGFOA2023

The Web



Surface Web

Google

YouTube

Instagram

Facebook

Deep Web

Medical Records

Legal Documents

Private Forums

Research Papers

Dark Web

Non-Indexed Content

Private Communication Forums

TOR

Illegal Activities

Illegal Trade

#FGFOA2023

Shady Shopping

Type of account	Average price log-in goes for on dark web
PayPal	$247
Costco	$5
ASOS (clothing)	$2
Airbnb	$8
Uber	$7
T-Mobile	$10.51
DHL	$10.40
Facebook	$5.20
Gmail	$1
Grubhub	$9

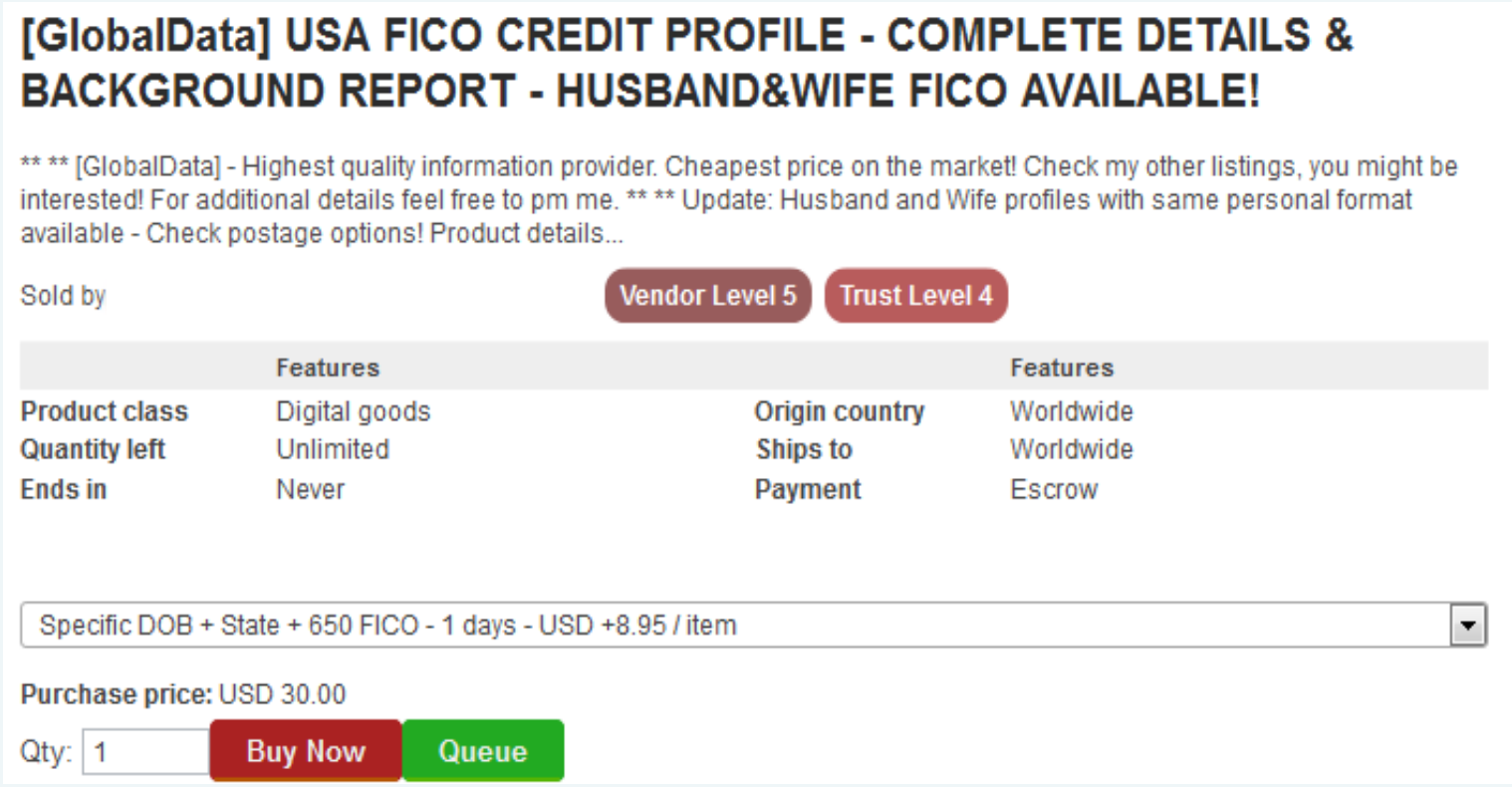
screenshot via MarketWatch.com

	Credit Card Data	Cloned Mastercard with PIN	$15
		Cloned American Express with PIN	$35
		Cloned VISA with PIN	$25
		Credit card details, account balance up to $1000	$12
		Credit card details, account balance up to $5000	$20
		Stolen online banking logins, minimum $100 on account	$35
		Stolen online banking logins, minimum $2000 on account	$65
		Walmart account with credit card attached	$10

Shady Shopping

Product	Price	Quantity
Remote control the phone of someone else, most new models supported	700 USD = 0.01286 ฿	1 X Buy now
Facebook and Twitter account hacking	500 USD = 0.00919 ฿	1 X Buy now
Other social network account hacks, for example reddit or instagram	450 USD = 0.00827 ฿	1 X Buy now
Full package deal, getting access to personal or company devices and accounts and searching for the data you need.	1800 USD = 0.03308 ฿	1 X Buy now
DDOS for protected websites for 1 month	900 USD = 0.01654 ฿	1 X Buy now
DDOS for unprotected websites for 1 month	400 USD = 0.00735 ฿	1 X Buy now
Hacking webservers, game servers or other internet infrastructure	1300 USD = 0.02389 ฿	1 X

Shady Shopping



[GlobalData] USA FICO CREDIT PROFILE - COMPLETE DETAILS & BACKGROUND REPORT - HUSBAND&WIFE FICO AVAILABLE!

** ** [GlobalData] - Highest quality information provider. Cheapest price on the market! Check my other listings, you might be interested! For additional details feel free to pm me. ** ** Update: Husband and Wife profiles with same personal format available - Check postage options! Product details...

Sold by Vendor Level 5 Trust Level 4

	Features		Features
Product class	Digital goods	**Origin country**	Worldwide
Quantity left	Unlimited	**Ships to**	Worldwide
Ends in	Never	**Payment**	Escrow

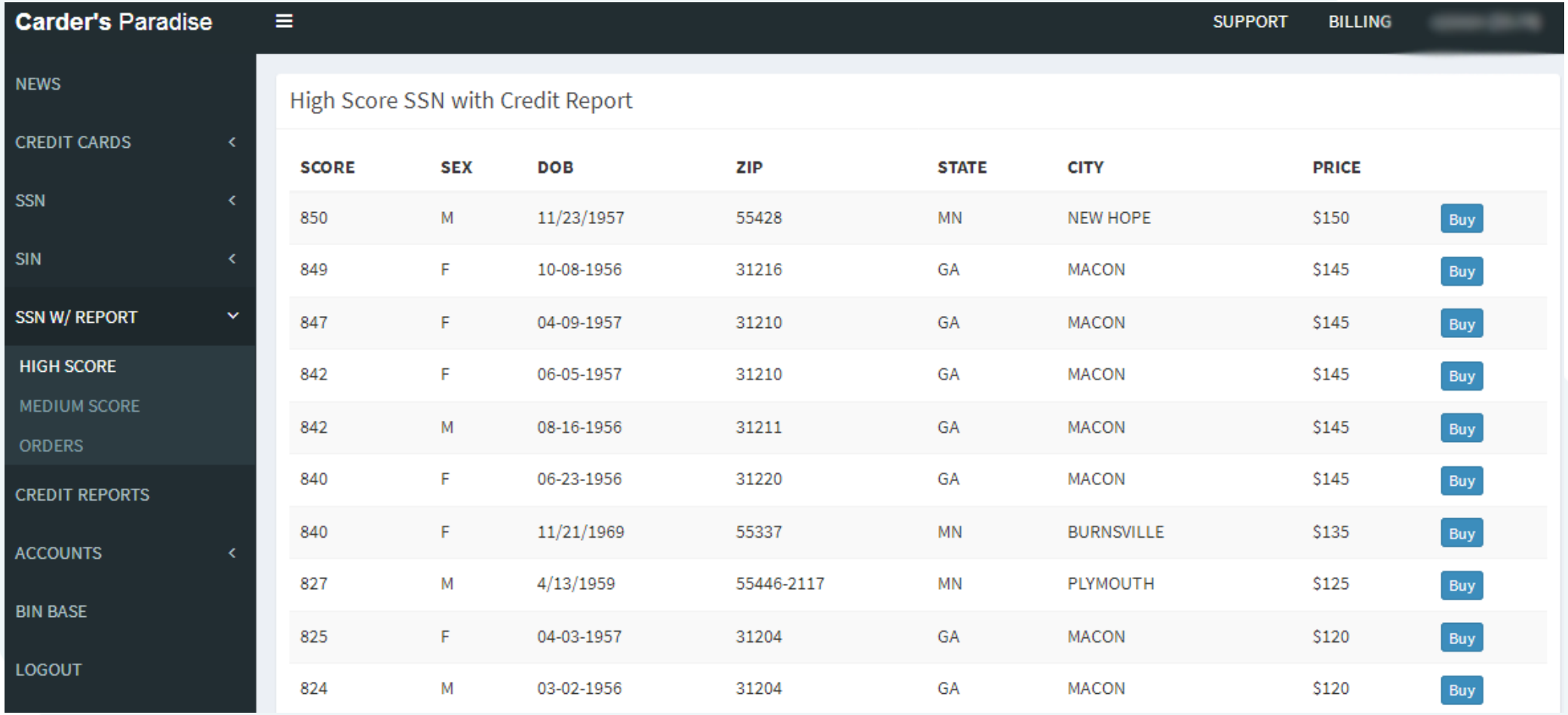
Specific DOB + State + 650 FICO - 1 days - USD +8.95 / item

Purchase price: USD 30.00

Qty: 1 Buy Now Queue

#FGFOA2023

The One Stop Shady Shop



SCORE	SEX	DOB	ZIP	STATE	CITY	PRICE	
850	M	11/23/1957	55428	MN	NEW HOPE	$150	Buy
849	F	10-08-1956	31216	GA	MACON	$145	Buy
847	F	04-09-1957	31210	GA	MACON	$145	Buy
842	F	06-05-1957	31210	GA	MACON	$145	Buy
842	M	08-16-1956	31211	GA	MACON	$145	Buy
840	F	06-23-1956	31220	GA	MACON	$145	Buy
840	F	11/21/1969	55337	MN	BURNSVILLE	$135	Buy
827	M	4/13/1959	55446-2117	MN	PLYMOUTH	$125	Buy
825	F	04-03-1957	31204	GA	MACON	$120	Buy
824	M	03-02-1956	31204	GA	MACON	$120	Buy

Risk Mitigation

Organizational security is all about defining and mitigating risks.

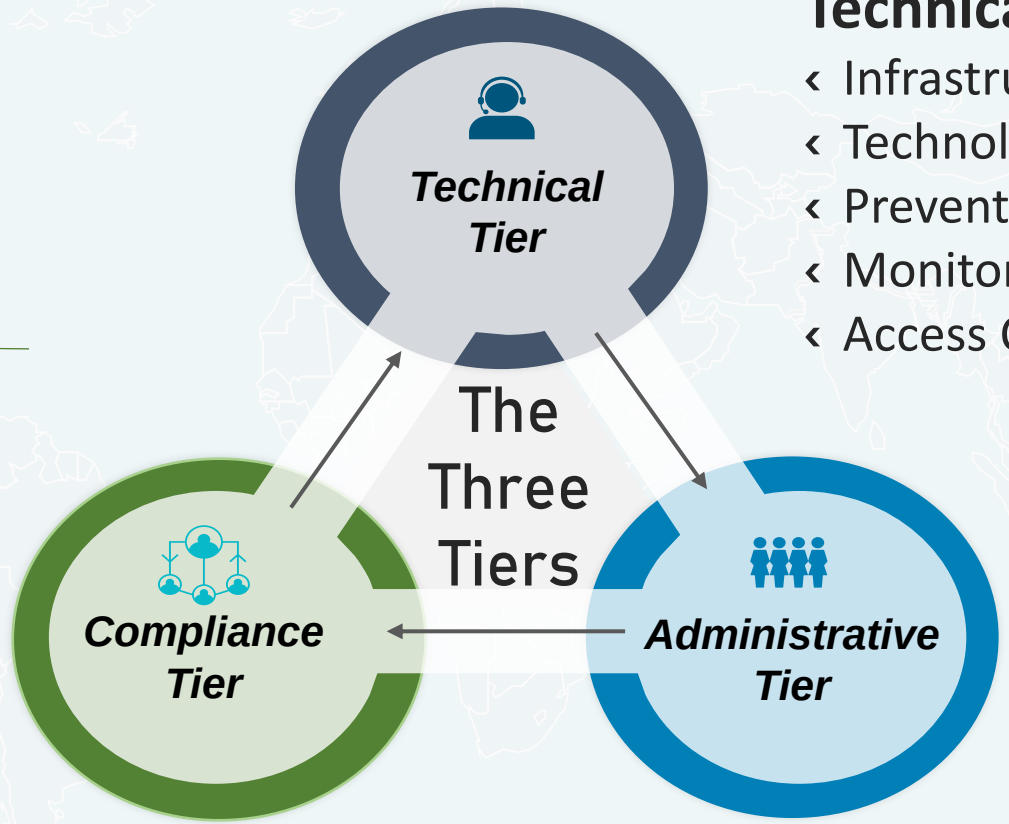
If we have limited time and resources, *where* and *how* we focus our efforts is the key.

Know Your Risks

Risk Register

#	Threat /Risk	City Impact?	Currently Mitigated?	Risk Factor	Suggested Priority	Notes
1	Account Takeover					
2	Advanced Persistent Threat					
3	Application Access Token					
4	Bill Fraud					
5	Business Invoice Fraud					
6	Brute Force Attack					
7	Compromised Credentials					
8	Credential Dumping					
9	Credential Reuse Attack					
10	Credential Stuffing					
11	Cloud Access Management					
12	Cloud Cryptomining					
13	Command and Control					
14	Cross-Site Scripting					
15	Cryptojacking Attack					
16	Data From Information Repositories					
17	DoS Attack					
18	DDoS Attack					
19	Disabling Security Tools					
20	DNS Amplification					

A Comprehensive Program



Technical

- Infrastructure
- Technology Based Defense
- Prevention Technology
- Monitoring Technology
- Access Controls

Compliance

- Due Diligence
- Due Care
- Reporting
- Audits
- Documentation
- Governance
- Accountability

Administrative

- Strategy
- Policies, Procedures
- Standards
- Planning
- Responsibilities

Security Controls

Data Identification & Management

Security Monitoring

Patch Management

Wireless (WIFI) Management

Mobil Device Management

Intrusion Detection/Prevention

Infrastructure Management

Backup and Recovery

Cloud Computing

Incident Response

Authentication

Mistake Management

Security Culture & Awareness

Risk Management

Policies & Procedures

Compliance Management

Governance & Oversite

User Access Management

Vulnerability Management

Access Control

Change Management

Application Security

Remote Access

Vendor Management

#FGFOA2023

Bad Odds

Data Identification & Management

Security Monitoring

Patch Management

Wireless (WIFI) Management

Mobil Device Management

Access Control

Intrusion Detection/Prevention

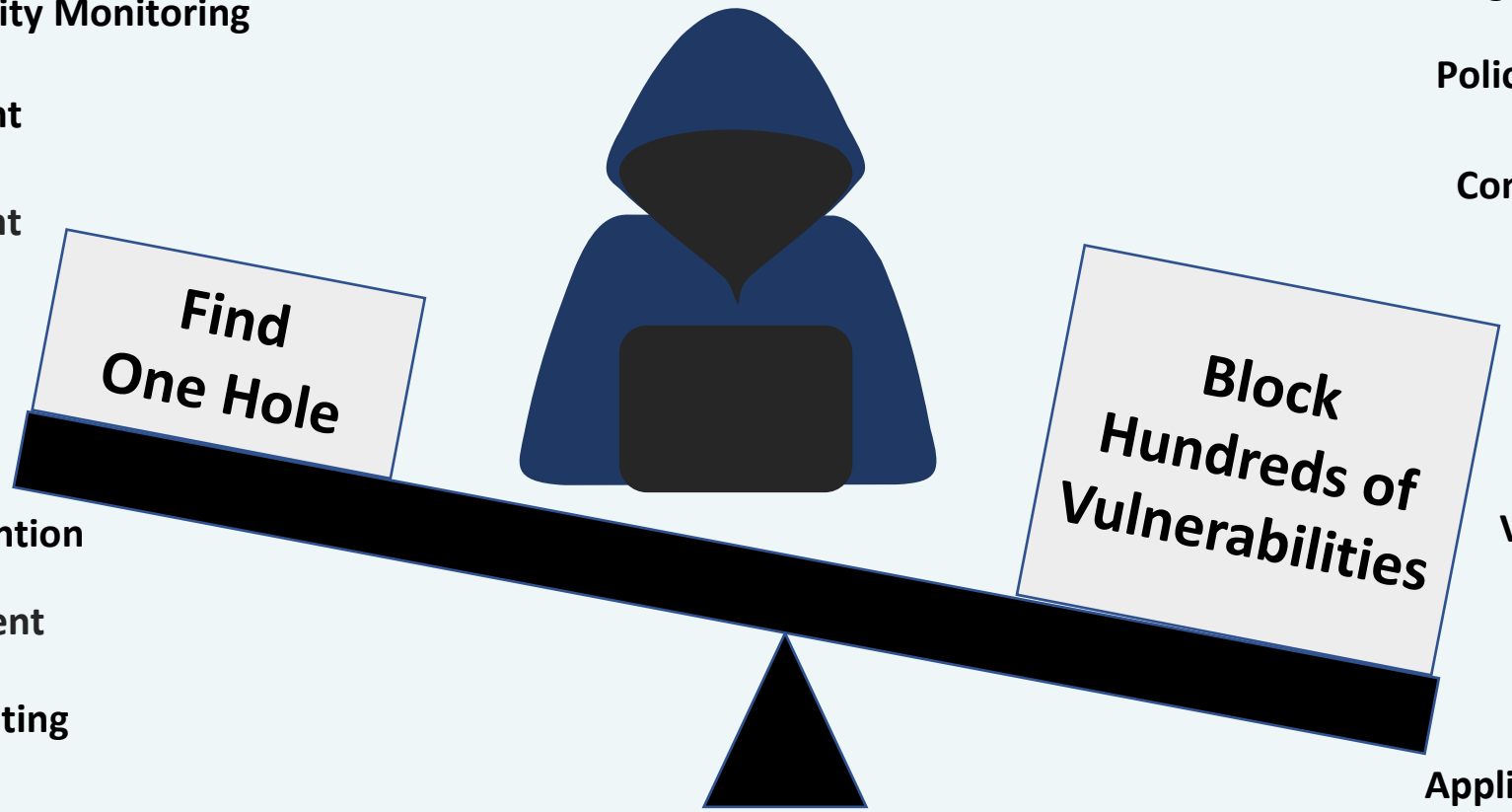
Infrastructure Management

Cloud Computing

Incident Response

Authentication

Mistake Management



Security Culture & Awareness

Risk Management

Policies & Procedures

Compliance Management

Governance & Oversite

User Access Management

Vulnerability Management

Change Management

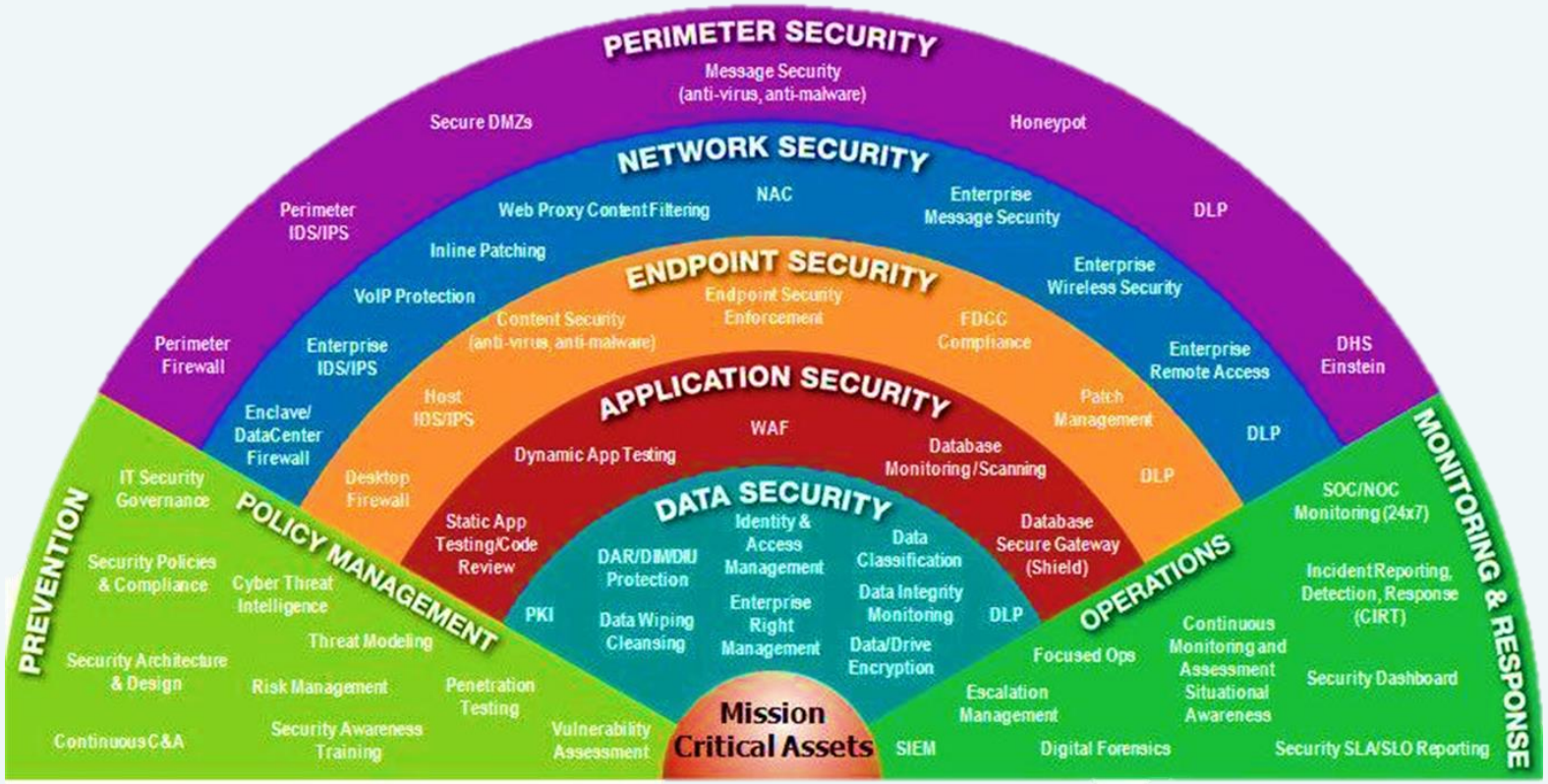
Application Security

Remote Access

Vendor Management

#FGFOA2023

Defense in Depth



Knowbe4 - https://blog.knowbe4.com/great-defense-in-depth-infographic

IT Finance Audit

Physical and Environmental Security

- Controls to ensure that physical access to facilities where IT equipment is kept is secure and restricted to authorized personnel

Logical Security - Granting, revising, and terminating logical access of personnel to network, financial applications, and related data

- Controls to ensure access is terminated as necessary on a timely basis
- Controls to ensure that only authorized personnel are granted access; access rights prevent assignment of incompatible duties, and privileges are revised as needed
- Controls to ensure Individuals with full administrative access to the network and financial applications do not have access to post transactions in financial applications
- Controls to ensure unique IDs and passwords are used to access network and financial applications

IT Finance Audit

Logical Security - Granting, revising, and terminating logical access of personnel to network, financial applications, and related data

- Controls to ensure that only authorized personnel are granted access; access rights prevent assignment of incompatible duties, and access is revised as needed

Data Backup and Recovery

- Controls to ensure that data is adequately backed up

Data Files, Business Rules, and Accounts

- Controls to ensure data or master files relevant to the audit are held and maintained securely
- Controls to ensure changes to data or master files are authorized, tested when applicable, reviewed, and documented

Reducing Liability

- ***Due Diligence*** is the act of continually investigating and understanding the risks and vulnerabilities the organization faces.
- ***Due Care*** is implementing security policies, procedures, standards, and countermeasures to protect from those threats.
- "If an organization does not practice due care and due diligence about the security of its assets, it can be legally charged with negligence and held accountable for any ramifications of that negligence" (Harris, 2010, p. 110)

CYA

Cover Your Assets

Need to Know

Risk Management

- Know and document your risks
- Look at the Finance big picture

Governance

- Be part of the organization's governance team
- Create your own Security Governance Finance team

Change Management

- Develop an internal change process
- Know how IT manages changes

Application Security

- Know what apps are in use, and what interfaces and data are generated

Data Management

- Classify sensitive data
- Know where this data is stored, how it is stored, and access levels

Access / Permissions

- Know the permission levels for applications
- Ensure proper permissions are granted

Mistake Management

- Understand where mistakes are likely to happen
- Implement polices and procedures

Incident Response

- Know what to do in case of an incident
- Train staff on incident reporting and handling

Vendor Management

- Document vendors, services, data, and security concerns
- Be on the lookout for social engineering

Remote Access

- Know remote access requirement
- Know what vendors can access
- Know what remote workers can access

Need to Know

Policies and Procedures
Document security-based policies and procedures

Compliance
Document compliance measures and compliance evidence

Security Awareness
Continual security awareness training

Question - 3

Which is not a best practice for managing data?

A. Control Access Permissions

B. Identify and Classify Sensitive Data

C. Know where and how data is stored

D. Multiple users sharing a single account

Question - 3

Which is not a best practice for managing data?

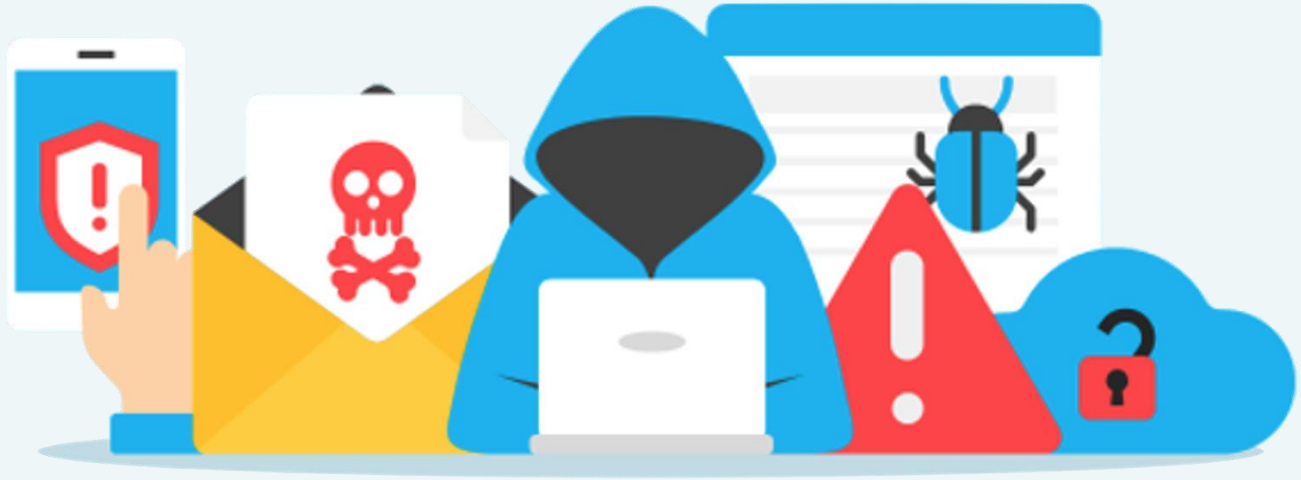
A. Control Access Permissions

B. Identify and Classify Sensitive Data

C. Know where and how data is stored

D. Multiple users sharing a single account

Information Protection



#FGFOA2023

Not My House

Protection

- Locked Doors
- Deadbolts
- Strong Doors
- Locked Windows
- Shatterproof Windows
- No Hidden Keys
- Few Keys Limited Distribution
- Security Cameras
- Security Alarm System
- Intrusion Detection
- Steal a Key
- Gated Community
- Security Guards

Easy Access Entry

- Unlocked Doors
- Unlocked or Open Windows
- Hidden Keys
- Accessible Chimney
- Try to Steal a Key
- Follow You In

Forced Entry

- Tool Kit
- Bypass Security Systems
- Pick Locks
- Bust Through the Door
- Break a
- Use Glass Cutter
- Force Through Any Opening
- Staying Out of Site

Not My Data

Protection

- Security Awareness Training
- Access Controls
- Continual Vulnerability Testing
- Continual Patching
- Intrusion Detection
- Intrusion Prevention
- System Monitoring and Alerts
- Policies and Procedures
- Issue Reporting and Management
- Continual Due Diligence
- Continual Due Care

Easy Access Entry

- Footprinting
- Discovering Known Vulnerabilities
- Discovering Holes in the System
- Stealing Credentials
- Buying Credentials
- Tricking via Social Engineering
- Phishing

Forced Entry

- Tool Kits
- Bypass Security Controls
- Exploit a Vulnerability
- Exploit an Application Weakness
- Exploit Unpatched Systems
- Brute Force

Crimes

Can Include:

- Stolen Money
- Fraud
- Productivity Losses
- Theft of Personal Data
- Embezzlement
- Post-attack Disruption
- Hacked Data and Systems
- Ransomware
- Destruction or Damage to Data
- Theft of Intellectual Property
- Financial Data Breaches

Creating A Culture of Security Awareness

Information/Cyber Security is Everyone's Responsibility

What You Don't Know Will Hurt You

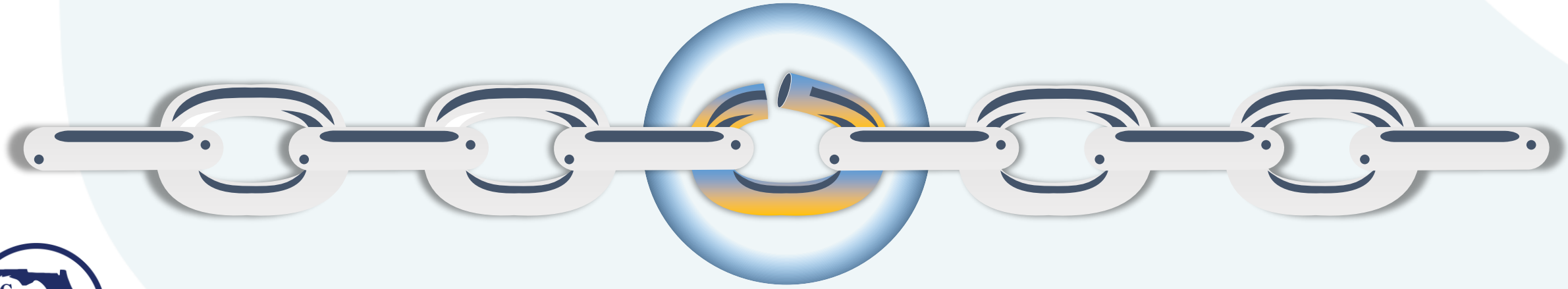
#FGFOA2023

Lack of Knowledge The Weakest Link

The Human Element

Humans are the weakest link in the security chain.

- Social engineering scams
- Phishing scams
- Human errors
- Human naivety
- Disgruntled employees
- Mistakes



No Easy Target

Security awareness is the knowledge and attitude that members of an organization possess regarding the protection of the physical, and especially informational, assets of that organization.

Lock the Car Doors

4th Question?

Who is responsible for cybersecurity in an organization?

A Organization Leaders

B Risk Management

C Information Technology (IT)

D Everybody

4th Question?

Who is responsible for cybersecurity in an organization?

A Organization Leaders

B Risk Management

C Information Technology (IT)

D Everybody

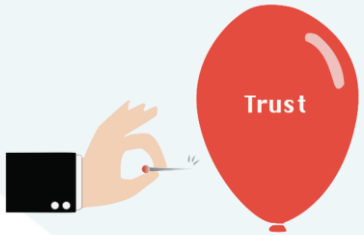
Pop the Bubble of Trust

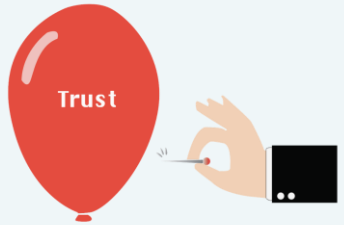
DANGER

ZERO TRUST ZONE

ZERO TRUST ZONE

DANGER





The Bad Actor's Best Friends

Take password protection for granted

Leave equipment unattended

Think it can't happen to them

Are naive and to trusting

Are easy prey

Ignore security practices

Click before they think

Think IT has it all taken care of

The Keys to the Kingdom

Handle your passwords with kids gloves and:

- Always change your password as required
- Always use complex passwords
- Never share your password
- Never write your password down
- Never use the same password for everything
- Use Dual Factor Authentication

Password Headache

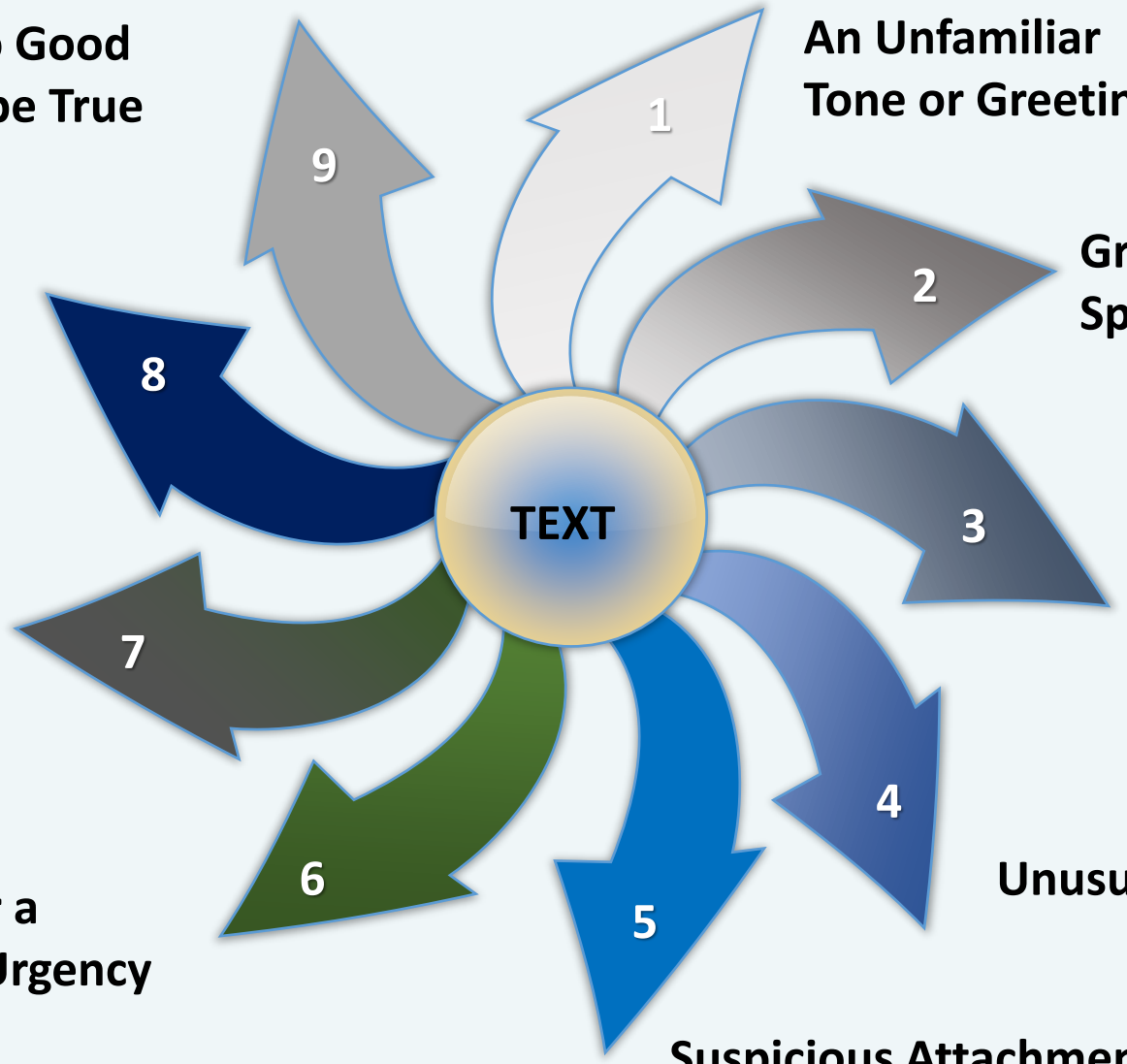
I forgot the password for the file where I keep all my passwords.

A Numbers Game

By blasting one phishing email, it is almost certain that someone will take the bait and:

- Open an infected attachment
- Click on an infected link
- Buy something that doesn't exist
- Give out confidential information
- Be gullible

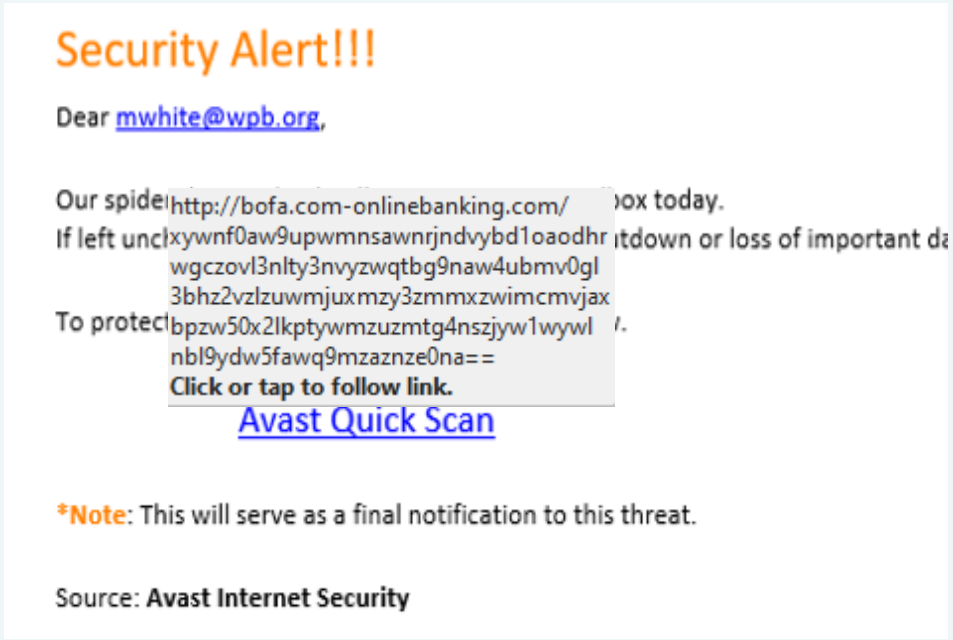
Phishing Email Red Flags

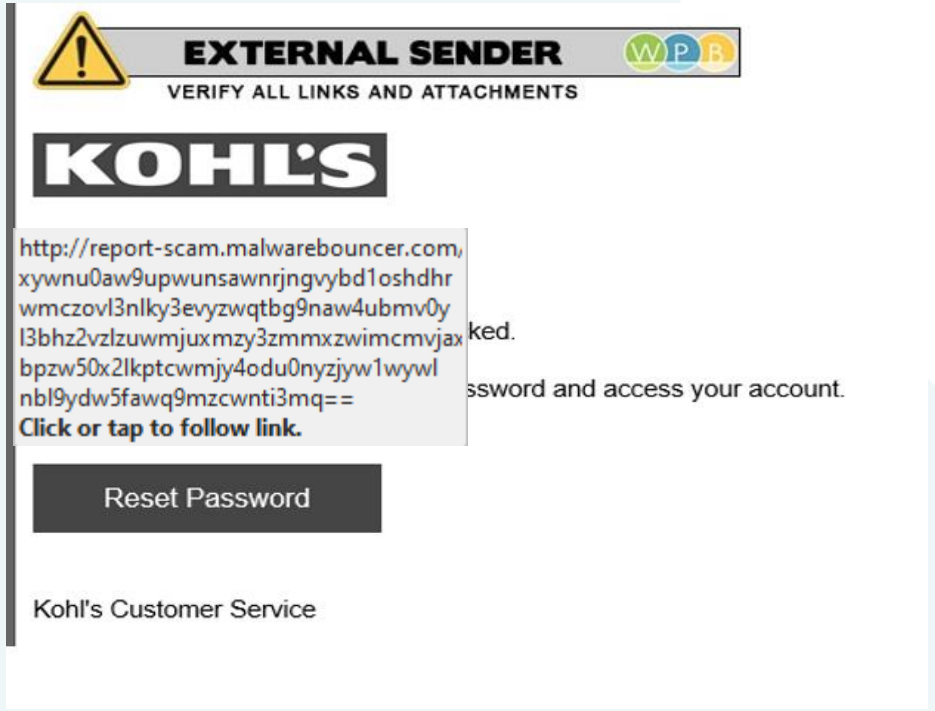


1. An Unfamiliar Tone or Greeting
2. Grammar and Spelling Errors
3. Inconsistencies in Email Addresses or Links
4. Unusual Requests
5. Suspicious Attachments
6. Threats or a Sense of Urgency
7. Just Doesn't Sound Right
8. You Did Not Initiate the Conversation
9. Too Good to be True

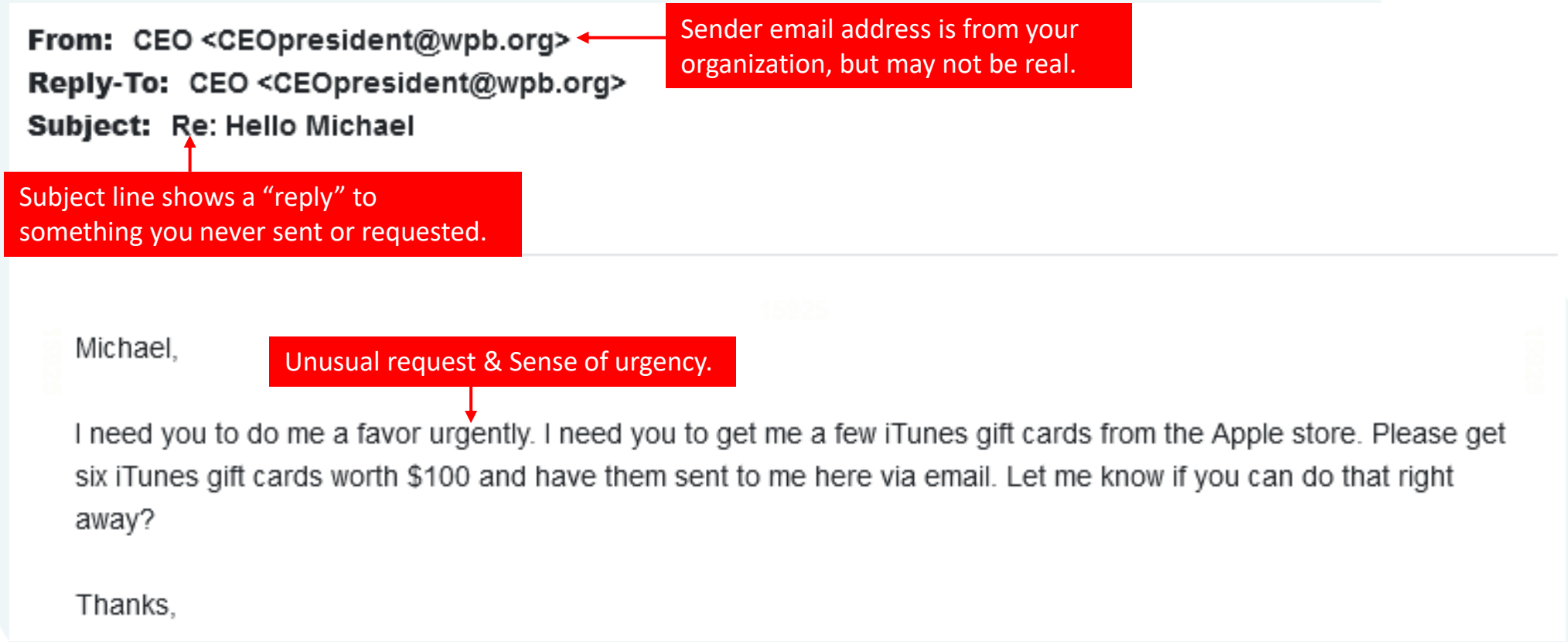
#FGFOA2023

Phishing Examples – Mouse Hover

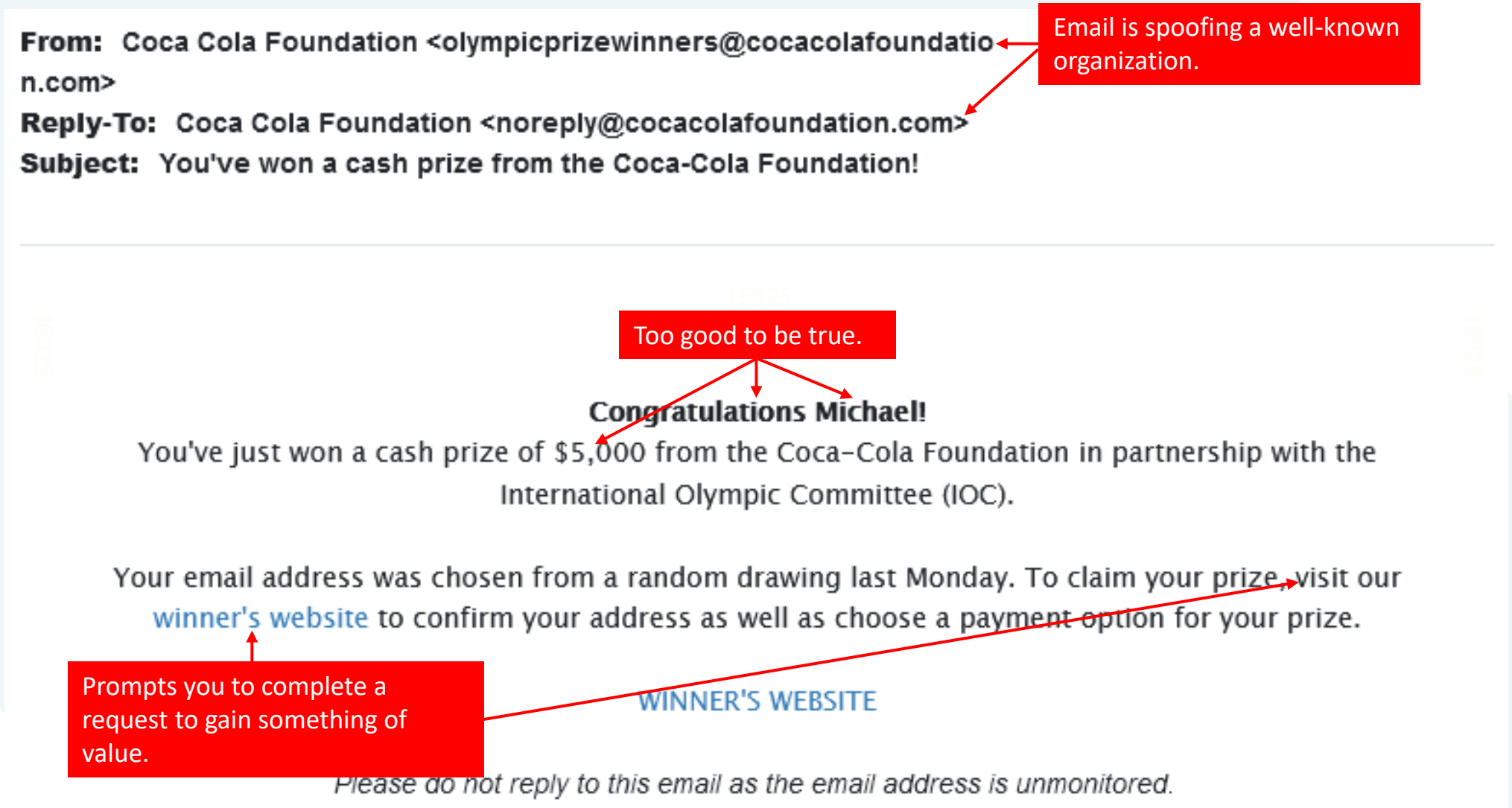




Examples: Urgent / Unusual Request



Examples : Too Good to be True



From: IT Department <it-department@wpb.org>
Sent: Monday, November 21, 2022 10:27 AM
To: Amado Yamasaki <ayamasaki@wpb.org>
Subject: Social Media Activity Reports

Not an email we use

Everyone,

We have recently noticed a high volume of social media posts containing inappropriate content. It is our goal to maintain a level of professionalism with our members and within our culture. The social media presence and image of or organization important, and as an extension of our organization, certain caution and care must go into what is posted on social media.

Please review your individualized social media report, and explain its content. Note that reports were created for all users and may not contain inappropriate material. Also, note that any flagged content created by social media friends of which yc are tagged in will also be present in these reports. Review by the **end of the day**.

To begin your review, access your report and authenticate with your network username and password using the link below:

Asking you to verify credentials

Social Media Content Reports

Thanks,

Dave Papadopoulos
Director - Information Technology
d.papadopoulous@wpb.org

Not the Director – We don't have a Director, we have a CIO

WEST PALM BEACH
Information Technology

Question - 5

Which of the following is not a Phishing Email Red Flag?

A Email is from someone you know

B Email creates a sense of urgency

C There are suspicious attachments

D Inconsistencies in email addresses or links

Question - 5

Which of the following is not a Phishing Email Red Flag?

A Email is from someone you know

B Email creates a sense of urgency

C There are suspicious attachments

D Inconsistencies in email addresses or links

Social Engineering

“You could spend a fortune purchasing technology and services…and your network infrastructure could remain vulnerable to old-fashioned manipulation.”

-Kevin Mitnick

It Sounded So Real

They sounded so legitimate

"Hello John, this is Bill from IT (Microsoft), and I am updating your computer right now, but I need your password to install these new much-improved applications for you. **You are going to love these new features!!!"**

No legitimate business or person will ever ask you for your password, credentials, or PII via text, email, or phone.

#FGFOA2023

Verify and Validate

USB Devices - If you are not positive where something came from, **DO NOT** connect it to your computer!!!

DO NOT let people you don't know work on your computer!!!

Social Engineering Attacks

- **Pretexting** – Creating a fake scenario
- **Phishing** – Sending out bait to fool victims into giving away their information
- **Fake Websites** – Modeled to look like the real thing so that a login with real credentials are now compromised
- **Fake Pop-up** – Pops up in front of the real website to obtain user credentials
- **Artificial Intelligence** – Used to predict behaviors and focus individualized attacks
- **Deepfakes – Fake audio and video that makes a person appear to be saying something they did not say**

Incident Reporting

Immediately report any suspected concern to your supervisor/manager/director or directly to the IT Help Desk

SEE SOMETHING

SAY SOMETHING

ONLY YOU CAN PREVENT BREACHES

#FGFOA2023

Security Awareness Basics

Take Password Protection Seriously

- Use complex passwords
- Don't write them down
- Change them frequently
- Don't share them

Never Give Out Personal Info

- No legitimate organization will ever ask you for personal information via email or phone

No Phishing Allowed

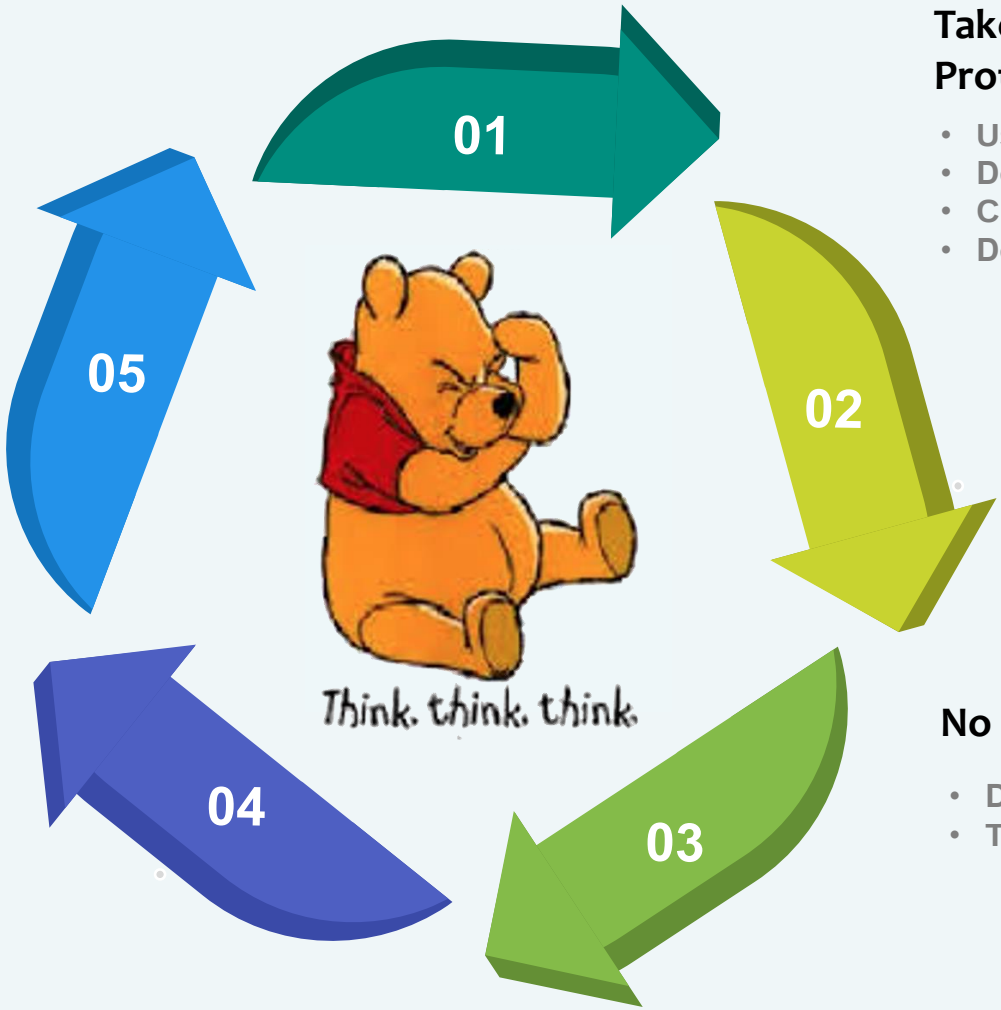
- Don't take the bait.
- Think twice before you click

See Something Say Something

- Immediately report any suspicious activity to your supervisor, manger, director or directly to the help desk

Pop the Bubble of Trust

- No trusting allowed
- Verify, verify, and then verify again
- If it sounds too good to be true, then it is



#FGFOA2023

Security Awareness Training Options

- Provide continual security awareness training and make it required
- Create security newsletters
- Perform continual social engineering and phishing tests
- Establish a departmental security team
- Establish peer groups
- Create a departmental security liaison
- Create a “See it - Say it” incident reporting program
- Add security updates and discussions to the departmental meeting agenda
- Reward and recognize good security actions and behaviors

It Happens Every Day

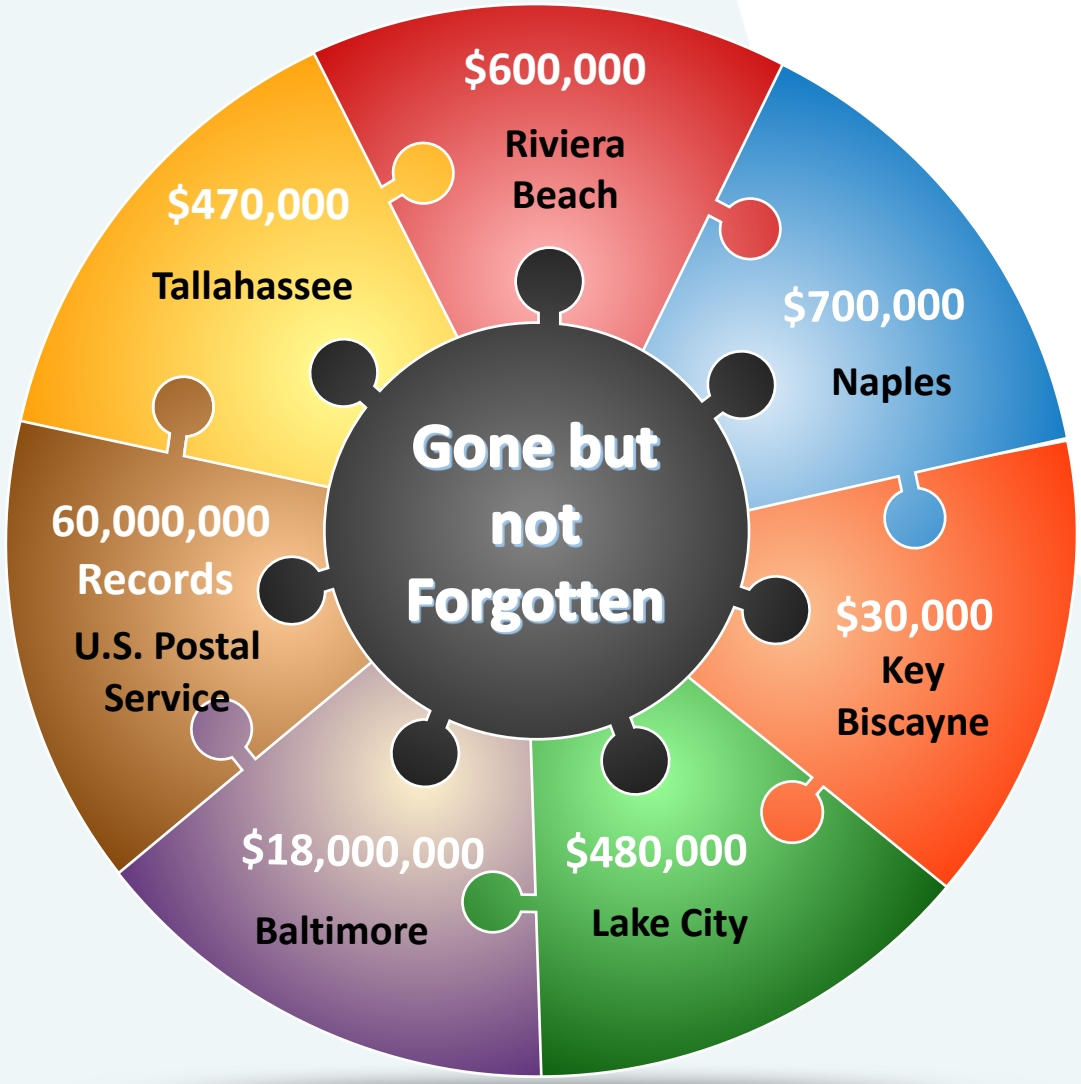
January 2023
Total: 25 entries
Affected industries: 20
Public sector: 8
Finance: 2

February 2023
Total: 34 entries
Affected industries: 23
Public sector: 11
Finance: 3

March 2023
Total: 38 entries
Affected industries: 24
Public sector: 10
Finance: 3

April 2023
Total: 17 entries
Affected industries: 16
Public sector: 7
Finance: 1

The Wheels of Misfortune



#FGFOA2023

The Must-Haves

- Establish strong senior leadership buy-in (make security important)
- Adequate FUNDING
- Develop robust governance and oversite (what you permit, you promote)
- Work with IT to validate and verify expectations
- Incorporate security in everything you do
- Know your data and identify sensitive data
- Know where and how sensitive data is stored
- Know who has access to your data and what permissions they have
- Don't take for granted everyone is doing what is needed
- Keep security "top of mind" for everyone
- Know your vendors and financial partners, and identify system access and data transfers
- Identify where mistakes can happen and mitigate risks
- Stay current with cyber security regulations
- Create departmental security policies and procedures, or add security sections to current policies and procedures
- Define compliance expectations
- Pop the "Bubble of Trust"
- Make security part of your culture

Question - 6

Which of the following is not a security program "must have?"

A Strong leadership buy-in

B Relying on IT to have everything taken care of

C Staying current with cyber security regulations

D Security Awareness Training and popping the "Bubble of Trust"

Question - 6

Which of the following is not a security program "must have?"

A Strong leadership buy-in

B Relying on IT to have everything taken care of

C Staying current with cybersecurity regulations

D Security Awareness Training and popping the "Bubble of Trust"

Questions?

#FGFOA2023

Thank You

References

Basset G., Hylender D., Langlois P., Pinto A., Widup S., & Kennedy D. (2022). *DBIR report 2022 – Introduction*. Verizon Business. https://www.verizon.com/business/resources/reports/dbir/2022/introduction/

Insurance Information Institute (2022). *Facts + statistics: Identity theft and cybercrime*. III. https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime

Knowbe4 - https://blog.knowbe4.com/great-defense-in-depth-infographic

KonBriefing Research - Cyber attacks USA 2022, 2023 | KonBriefing.com