

RAYMOND JAMES



SECURITY AWARENESS

# An Inside Look at Cybersecurity

CURRENT THREATS, DEFENSE CAPABILITIES & KEY RECOMMENDATIONS

Chuck Sapp | May 30, 2024

**RAYMOND JAMES**

# An Inside Look at Cybersecurity

- I. CURRENT ENVIRONMENT
- II. ATTACK VECTORS
- III. INFORMATION SECURITY STRATEGY
- IV. CORE CAPABILITIES
- V. KEY RECOMMENDATIONS
- VI. QUESTION & ANSWER

# CURRENT ENVIRONMENT

AN EVER-CHANGING AND GROWING REALITY

## CURRENT ENVIRONMENT | Cyberattacks In The News

T-Mobile, Verizon workers get texts offering \$300 for SIM swaps

**Hackers Breached Colonial Pipeline Using Compromised Password**

**MGM Resorts confirms hackers stole customers' personal data during cyberattack**

**Researchers find dozens of fake E-ZPass toll websites after FBI warning**



**180k Impacted by Data Breach at Michigan Healthcare Organization**

Mr. Cooper

**Cyber Attack**

Render Online

Payment Services

Unavailable

**Roku Says 576,000 Accounts Compromised In Latest Security Breach**

# Social Engineering

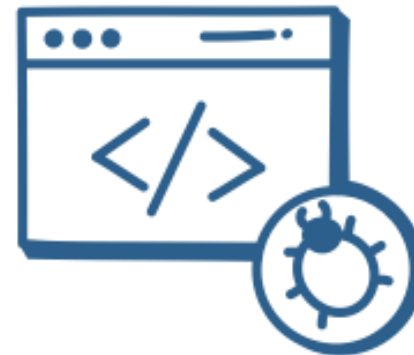
Social engineering refers to the various methods that **cybercriminals** use to **exploit human behavior**. It's about taking advantage of our **natural tendencies** to **deceive** or **coerce users** into performing certain actions, such as:



Giving up account credentials



Handing over sensitive data



Running malicious code



Transferring funds

**Emotions:** Urging action, sparking excitement, or instilling fear of loss.

**Trust:** Impersonating trusted individuals or exploiting reputable brands.

**Fatigue:** Exploiting tired or distracted users for emotion-driven decisions.



# Telephone-Oriented Attack Delivery (TOAD)

Telephone-Oriented Attack Delivery is a tactic where fraudsters **exploit phone communication** to **manipulate individuals** into divulging **confidential information** or performing actions that **compromise security**.



Email  
Received



Victim Dials  
Provided  
Number



Fraudster  
Answers  
Call



Fraudster  
guides to  
site/software



Fraudster  
Directs  
Victim to  
Malicious  
Download



Fraudster  
Gains  
Access

**Tech Support Scams, Banking Scams, Refund Scams, Lottery or Prize Scams, IRS/Tax Scams**

# ATTACK VECTORS

THE AMPLIFYING EFFECTS OF SOCIAL ENGINEERING

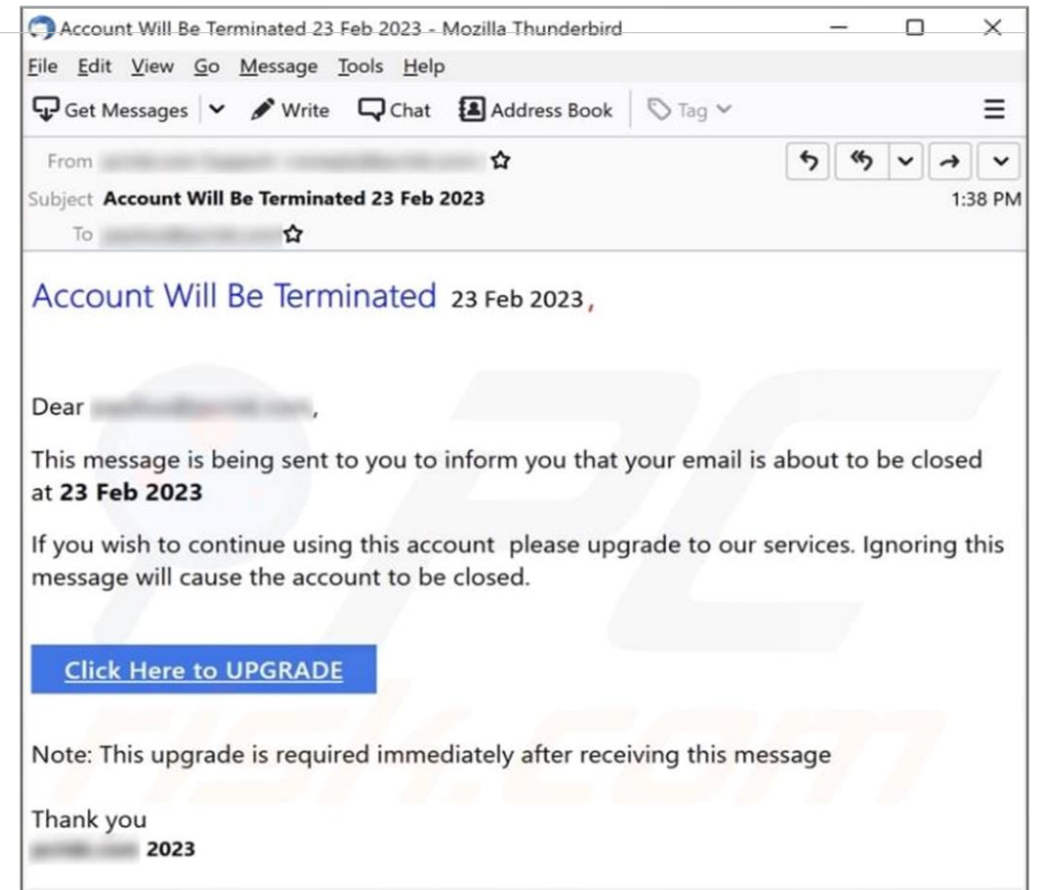
# ATTACK VECTORS | Social Engineering

## Phishing Emails

- Conveys a sense of urgency
- Typos and alternate spelling
- From a person of authority
- Reply address does not match the sender address

## Best Practices

- Remember that unsolicited emails are suspicious emails

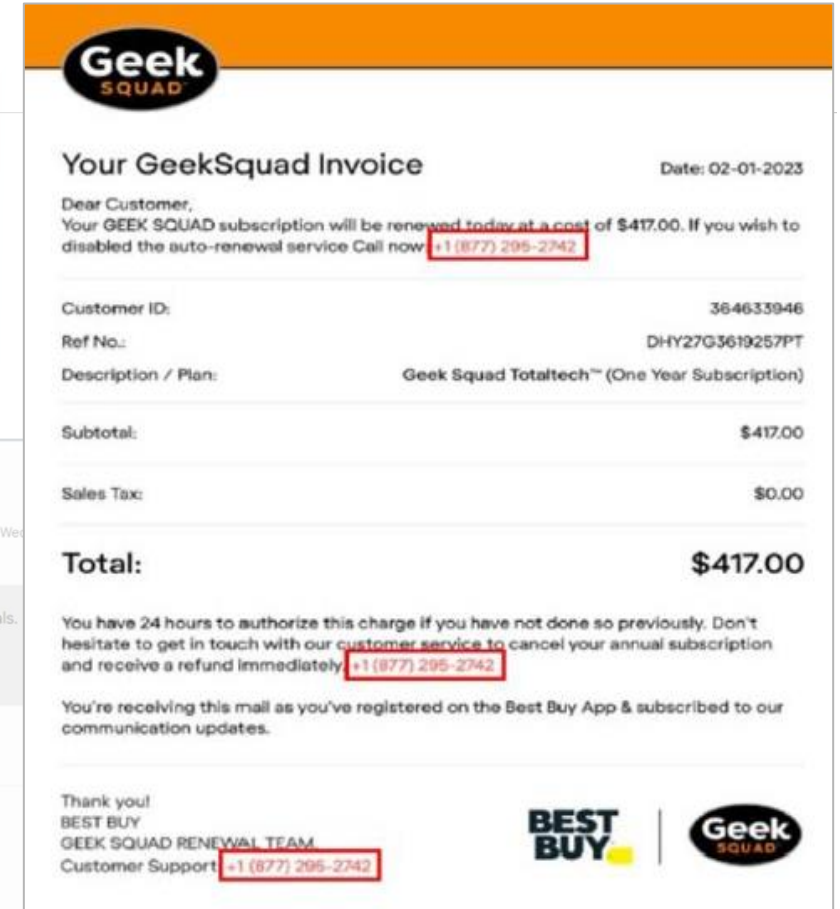
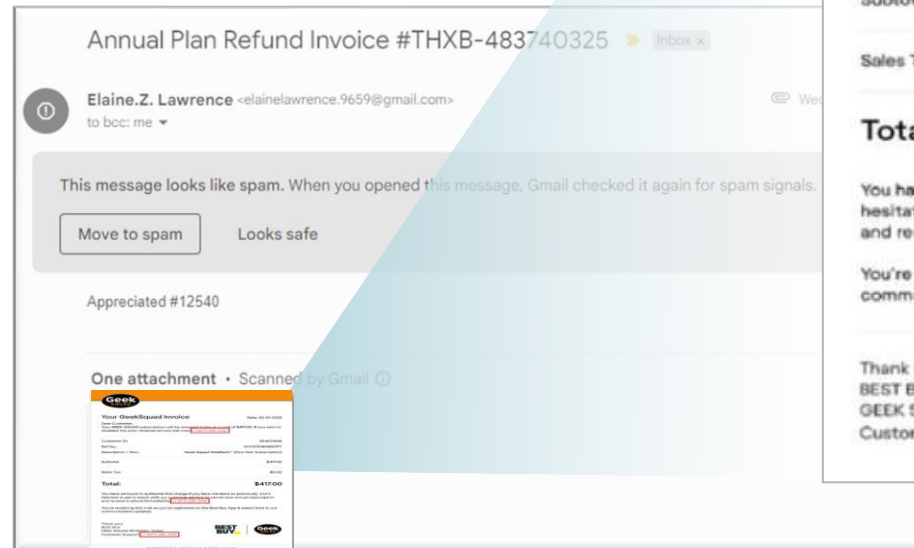




# ATTACK VECTORS | Social Engineering

## Tech Support Scams

- Avoid anti-virus/threat detection
- Bypass Email Filters that base threats off a malicious link



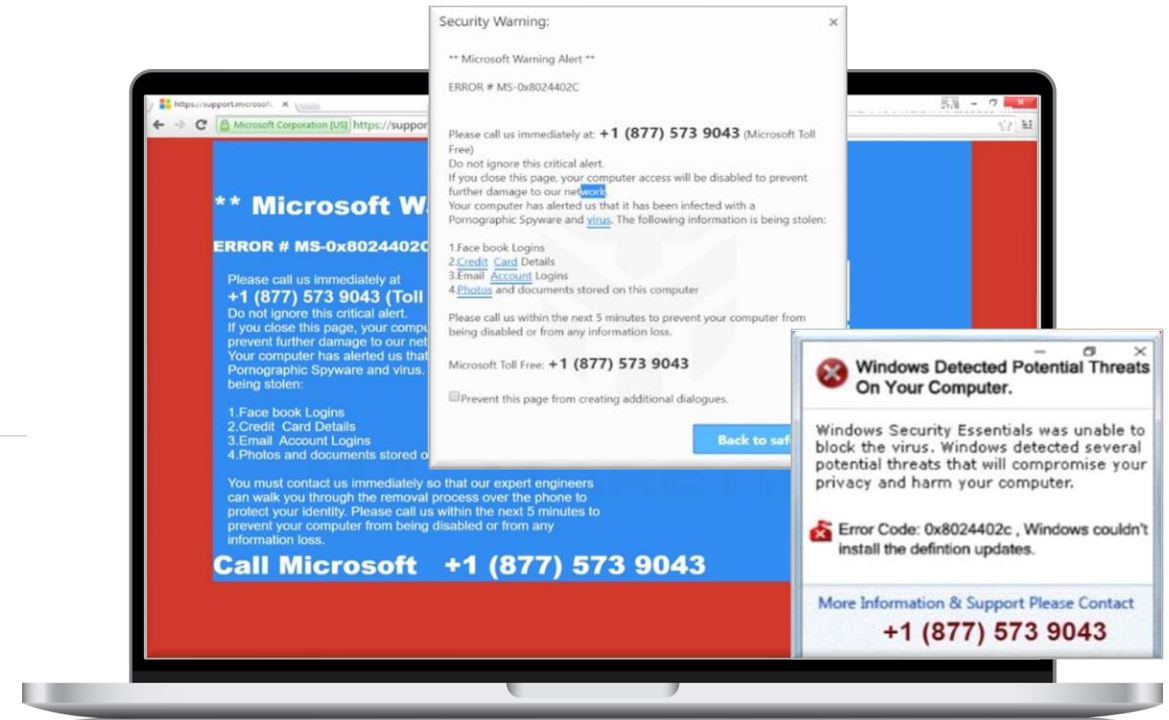
# ATTACK VECTORS | Social Engineering

## Tech Support Scams

- Urgent or alarming messages, pressuring you to act immediately.
- Requests for remote access to your device.
- Asking for payment via gift cards, wire transfers, or other non-traditional means.

## Best Practices

- Never provide personal, financial, or computer information to unsolicited requests.
- Never allow remote access to your computer unless you're certain of the individual's identity and legitimacy.



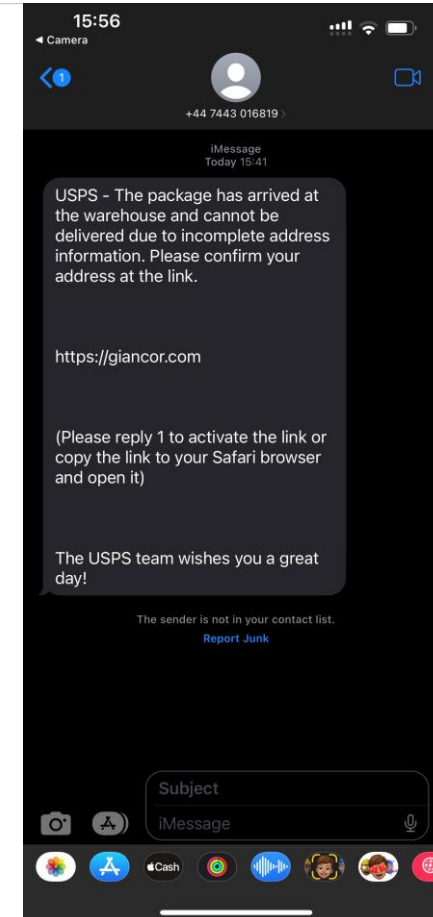
# ATTACK VECTORS | Social Engineering

## Smishing

- Messages appear to be from common and widely used source
- May cite a need to rectify some kind of billing or urgency

## Best Practices

- Don't tap on links
- Go to source directly if you legitimately have business the company referenced
- Block the texter



# ATTACK VECTORS | Social Engineering

## Vishing & Spam Calls

---

- Scam callers will spoof legitimate numbers or buy phone blocks to bypass Spam Filters

## Best Practices

---

- Never provide personal, financial, or computer information to unsolicited requests
- Never allow remote access to your computer unless you're certain of the individual's identity and legitimacy.
- Do not engage with scam calls, just hang up.
- Don't assume that because someone has your number, they mean well.
- Report scam calls to the FCC Consumer Complaint Center



# Number 1

Complaint received by the  
Federal Communications  
Commission (FCC)

---



# 50 Billion

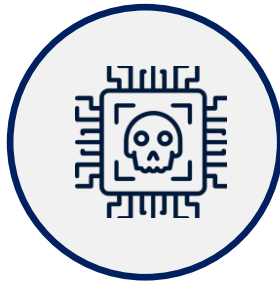
Estimated scam calls in 2021

# CURRENT ENVIRONMENT | Ransomware

## Ransomware

---

Ransomware is a type of malicious software that blocks access to a computer system until a sum of money is paid. It has evolved into a big business in the cybercrime world.



**Encryption for Ransom:** Some ransomware attacks involve encrypting the victim's data and then selling them the key to decrypt it.



**Data Theft and Exposure:** In other cases, attackers steal the data and threaten to expose it unless a ransom is paid.



**Ransomware as a Service (RaaS):** A business model where developers sell their malware to hackers, who use it to carry out their own attacks.

# INFORMATION SECURITY STRATEGY

A COMPREHENSIVE APPROACH



# RJF INFORMATION SECURITY | Strategy

## A Multi-Faceted Approach to Cybersecurity



### PROTECT

- Best protective measures available
- Creative solution design and engineering
- Life cycle management of solutions



### DETECT

- Assume protective measures may fail
- Real-time detection of anomalous activity
- Situational awareness: environment, threats and RJ businesses.



### DEVELOP

- Build relationships based on trust and teamwork
- Invest in technical training, cross-training and leadership development
- Hire great talent that fits our high-performing team culture



### PARTNER

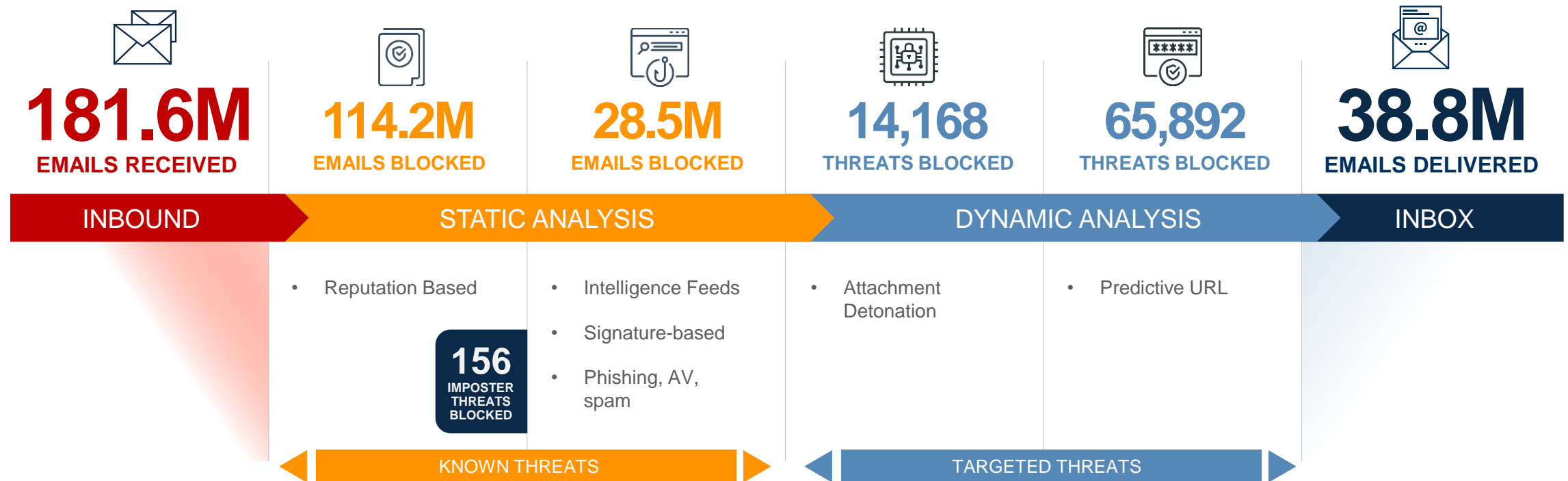
- With third parties (e.g., vendors, government, universities)
- With RJF businesses and RJF partners
- With RJ IT

# CORE CAPABILITIES

TESTED, REDUNDANT & LAYERED

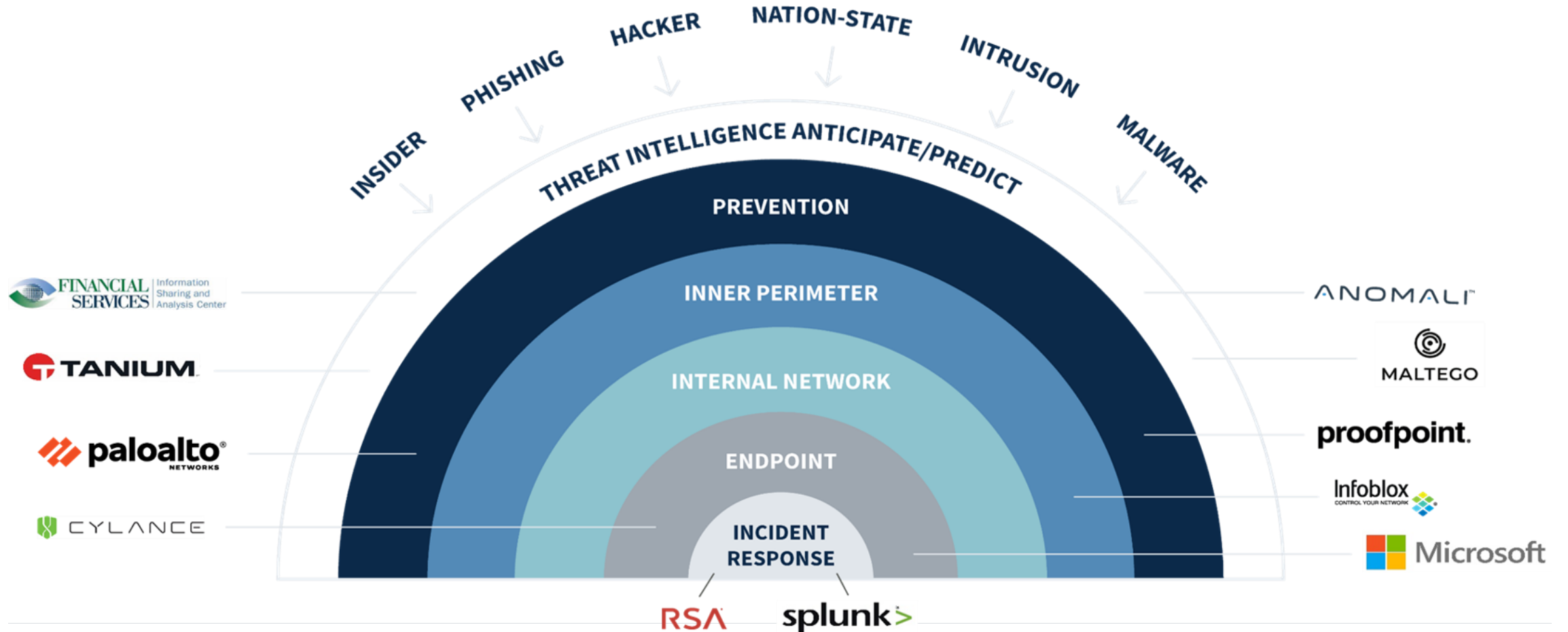
# CORE CAPABILITIES | State-of-the-Art Defenses

Email protection on a major scale



# CORE CAPABILITIES | Defense in Depth

Layered protections and security controls across the enterprise



# Key Capability: Cyber Threat Center (CTC)



- Real-time, **24/7/365** monitoring
- Staffed by **certified** information security analysts
- **750 billion** log events each year
- **50,000 per second** during peak business hours



24-hour coverage from: St. Petersburg, Florida | London, England | Vancouver, Canada



# CORE CAPABILITIES | Cyber Threat Center (CTC)

State of the art monitoring and detection capabilities





# KEY RECOMMENDATIONS

TAKE THESE STEPS TO PROTECT YOUR INFORMATION

# KEY RECOMMENDATIONS | Enhanced Authentication for Client Access


## The most effective means to prevent fraud & identity theft from stolen credentials

- Mandatory security feature moving forward
- Provides two-factor authentication

### Security Verification | Enhanced Authentication

#### Select Delivery Method

Select the phone number and method to receive the authentication code and click Next. You will enter the code on the next screen.



Phone Number  
XXX-XXX-3681

Text - Mobile only  
 Phone

Note: We don't charge for text messages sent to your mobile device; however, standard message and data rates may apply. If you select voice and your number requires an extension, we won't be able to reach you.

Remember me on this computer

What you should know.

If you want to receive a phone call to get the authentication code, the phone number cannot include an extension.

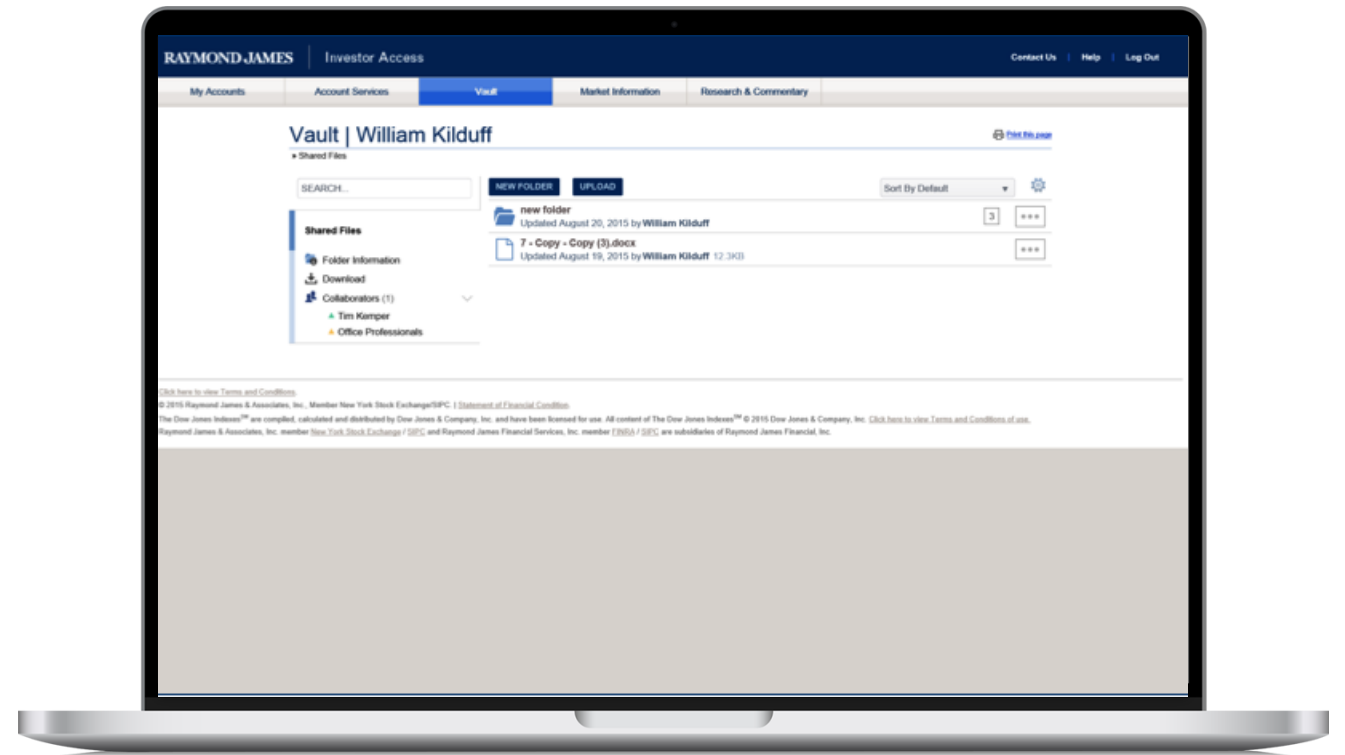
If the phone number you select is no longer valid, you won't be able to receive the verification code to complete the process (The phone numbers shown for you reflect our current records).

Please contact your Advisor or Investor Access Support at 877-RJ-ACCESS (877-752-2237) if you need assistance.

# KEY RECOMMENDATIONS | Vault

## A secure online tool to exchange, organize and store important files

- Clients have access directly from the Client Access homepage
- Fully encrypted and equipped with enhanced security features, including malware detection and data leakage monitoring



# KEY RECOMMENDATIONS | Personal Protective Measures

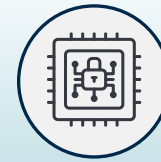
## Establish your personal security perimeter



Consistently update software to quickly address and patch known vulnerabilities.



Treat every unexpected email with caution, avoiding unknown links.



Prioritize encrypted communications, especially with SSL/TLS, for secure data exchange.



Store devices securely when unattended and regularly back up files to cloud or external drives.



Only install trusted apps, granting minimal required permissions.



Regularly check and update firewall settings on your devices.



Set your antivirus for automatic updates and scans.



Avoid downloading from untrusted sources and practice safe web browsing habits.



Use strong, unique passwords and employ a password manager for optimal security.

# KEY RECOMMENDATIONS | Password Strength

2020	TIME TO CRACK
10 CHARACTERS	5 YEARS
11 CHARACTERS	400 YEARS
12 CHARACTERS	34k YEARS
13 CHARACTERS	2m YEARS
14 CHARACTERS	200m YEARS
15 CHARACTERS	15bn YEARS
<b>16 CHARACTERS</b>	<b>1 Trillion YEARS</b>
17 CHARACTERS	93tn YEARS
18 CHARACTERS	7qd YEARS

4-5: Instantly 6: Seconds 7: Minutes, 8: Hours 9: Weeks

2023	TIME TO CRACK
10 CHARACTERS	2 WEEKS
11 CHARACTERS	3 YEARS
12 CHARACTERS	226 YEARS
13 CHARACTERS	15k YEARS
14 CHARACTERS	1m YEARS
15 CHARACTERS	77m YEARS
<b>16 CHARACTERS</b>	<b>5 Billion YEARS</b>
17 CHARACTERS	380bn YEARS
18 CHARACTERS	26tn YEARS

4-6: Instantly 7: Seconds 8: Minutes, 9: Hours



Characters: Numbers, Symbols, Upper and Lowercase Letters

# YOUR SECURITY IS OUR PRIORITY

At Raymond James, we believe that putting clients' needs first – including their need for security – is the best way to ensure their success and, in turn, the success of the firm. Our guiding principles have led us to over 144 quarters of continuous profitability. The integrity, strength and stability at the foundation of the firm offer the most important protection for your accounts. And we back our efforts with a pledge you can believe in.



We want you to have the highest level of confidence in doing business with us. That's why we offer you this assurance:

We will reimburse you for actual losses in any of your Raymond James accounts due to unauthorized access to a Raymond James system that occurs through no fault of your own.





# THANK YOU

## Questions & Answer

INTERNATIONAL HEADQUARTERS: THE RAYMOND JAMES FINANCIAL CENTER  
880 CARILLON PARKWAY // ST. PETERSBURG, FL 33716 // 800.248.8863  
RAYMONDJAMES.COM

---

© 2023 Raymond James & Associates, Inc., member New York Stock Exchange/SIPC.  
Raymond James® is a registered trademark of Raymond James Financial, Inc.