



**Us
And
Our
Staff**



security@falconi.com
220 Gardenpoint Plaza, Suite 205, Newark, NJ 0710
(973) 555-1490

CHARTER REFERENCE

For Approval By: Chief Information Officer (CIO)

Version: 1.0

1. Purpose & Mission Statement

At Falconi, our mission is to empower our NFL clients at every stage of their careers, offering guidance in providing excellent representation, strategic career development, and support on and off the field at every turn.

We help our clients navigate their high-profile status, their finances, and manage their endorsements.

Our purpose is to serve as a trusted partner to all our athletes. We are committed to maximizing our clients' potential through our world-class expertise in contract negotiations, marketing opportunities at a global scale, and one on one mentorship at the highest level. We aim to cultivate a role that extends far beyond the field. We want to protect, guide, and help our clients through every transition in their careers.

2. Scope

The Cybersecurity Program applies to:

- **Digital Asset Protection**
 - **Ensuring the security of our clients' personal, financial, and professional data across our platforms**
- **Risk Management**
 - **We need to identify and mitigate any cybersecurity threats that are unique to our industry, targeting our athletes with all devices and social media accounts**
- **24/7 Threat Monitoring**
 - **Offering 24/7 threat monitoring of all activity to detect and respond to unauthorized access and potential data breaches**
- **Education and Cybersecurity Awareness**



security@falconi.com
220 Gardenpoint Plaza, Suite 205, Newark, NJ 0710
(973) 555-1490

- Equipping our clients and our teams with knowledge and best practices to help our team avoid cyber threats at all times
- Incident Response
 - Providing rapid-response protocols for any data breaches, compromised accounts, and threats foreseen to minimize damage done to the company

3. Authority

The cybersecurity team operates under the authority granted by executive leadership and reports functionally to the Chief Information Security Officer (CISO). The team is authorized to:

- Access all necessary systems and logs for security monitoring
- Enforce cybersecurity policies and standards
- Conduct security assessments and audits
- Investigate and respond to a security incident
- Provide recommendations to mitigate identified risks

4. Responsibilities

The cybersecurity program will

- Develop and maintain the cybersecurity policy framework
- Conduct regular risk assessments and vulnerability scans
- Manage incident response and recovery procedures
- Provide employee security awareness training
- Monitor compliance with internal policies and external regulations (e.g., NIST, ISO, GDPR)
- Ensure business continuity and disaster recovery planning from a security perspective

Signatures

Chief Information Security Officer (CISO)



security@falconi.com
220 Gardenpoint Plaza, Suite 205, Newark, NJ 0710
(973) 555-1490

Name:

Signature: _____

Date: _____

Chief Information Officer (CIO)

Name: _____

Signature: _____

Date: _____

Awareness Training Video and Quiz

Training Video:

https://drive.google.com/file/d/18C1Ys2F1V_O4JbIHT71m71rdcur2HiMI/view

Training Slideshow / Quiz:

<https://www.canva.com/design/DAGp-ABSbW4/SCjtqdyI9fBMf-XUEzjY-g/edit>



security@falconi.com
220 Gardenpoint Plaza, Suite 205, Newark, NJ 0710
(973) 555-1490



Cybersecurity Checklist Onboarding

1 COMPANY MISSION & POLICY ACKNOWLEDGEMENT		
• I have reviewed Falconi's mission & Cybersecurity Charter.		<input type="checkbox"/>
• I have acknowledged Falconi's Acceptable Use Policy (AUP).		<input type="checkbox"/>
• I have completed Falconi's Awareness Training Plan.		<input type="checkbox"/>
2 SYSTEM ACCESS & SECURITY SETUP		
• I have integrated my Falconi email with MFA (Okta).		<input type="checkbox"/>
• I have created a unique default password according to Falconi password standards (12+ characters, symbols, etc).		<input type="checkbox"/>
3 PHISHING & THREAT AWARENESS		
• I have read Falconi's phishing awareness resources.		<input type="checkbox"/>
• I have completed Falconi's Phishing Simulation Training.		<input type="checkbox"/>
4 DEVICE & DATA HANDLING PROCEDURES		
• I have completed the "Clean Desk" and lock screen policies Training Module.		<input type="checkbox"/>
• I understand "Clean Desk" and lock screen policies.		<input type="checkbox"/>
• I understand it is my duty to recognize and report security incidents or suspicious activities.		<input type="checkbox"/>
5 INCIDENT RESPONSE		
• I have bookmarked the Falconi Incident Response Form and Reporting Hotline on all work devices.		<input type="checkbox"/>
• I have reviewed Falconi's incident escalation path and understand when to report an incident.		<input type="checkbox"/>
6 CONFIDENTIALITY		
• I understand that player information, contracts, and scouting reports are confidential. I will not discuss any of this with unauthorized parties, regardless if they are employees of Falconi.		<input type="checkbox"/>

EMPLOYEE SIGNATURE:

DATE:



security@falconi.com
220 Gardenpoint Plaza, Suite 205, Newark, NJ 07102
(973) 555-1490



security@falconi.com
220 Gardenpoint Plaza, Suite 205, Newark, NJ 0710
(973) 555-1490

Phishing Simulation

We executed a multi-phase phishing simulation to establish baseline user susceptibility, test technical delivery methods, and reinforce security awareness.

Development & Execution Summary

1. Link Design: Created a disguised phishing link using Short.io, styled to appear as a Google Docs invite with a generic document title to reduce suspicion.
2. Delivery Method: Posted casually in a shared Discord server with a “join the document” prompt to simulate an impulsive click scenario.
3. Deception Technique: Leveraged Discord’s inline link preview to hide the real URL and increase plausibility, mimicking real-world phishing behavior.
4. Results: 4/6 interns (66%) clicked the link within 10 minutes, confirming user susceptibility and validating link realism.
5. Outcome: Established baseline phishing vulnerability data, justifying escalation to a controlled HTML-based email campaign.

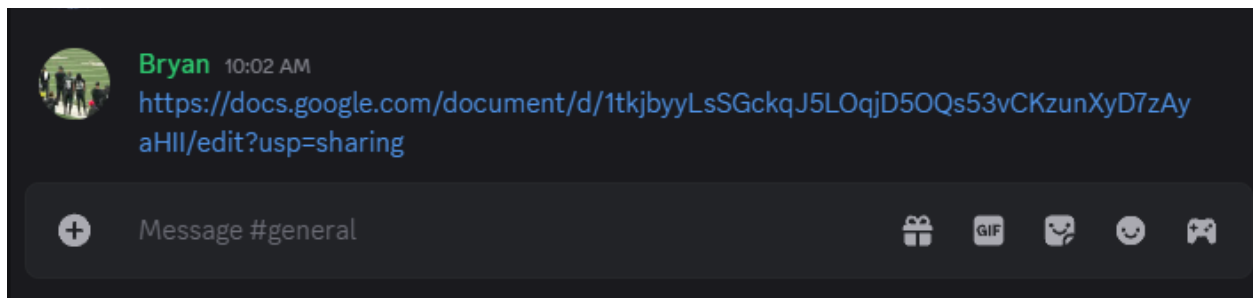


Figure 1: Initial Discord Phishing Simulation Message

Email Clone Development:

1. Created custom HTML/CSS clones of Google Docs invite email for more realistic phishing appearance.
2. Some JS and advanced styling failed in certain email clients, this was resolved by embedding image assets via Imgur links storing image links in the email itself.
3. Sent emails using Thunderbird, ensuring proper HTML rendering in inboxes.



security@falconi.com
220 Gardenpoint Plaza, Suite 205, Newark, NJ 0710
(973) 555-1490

Code Snippet:

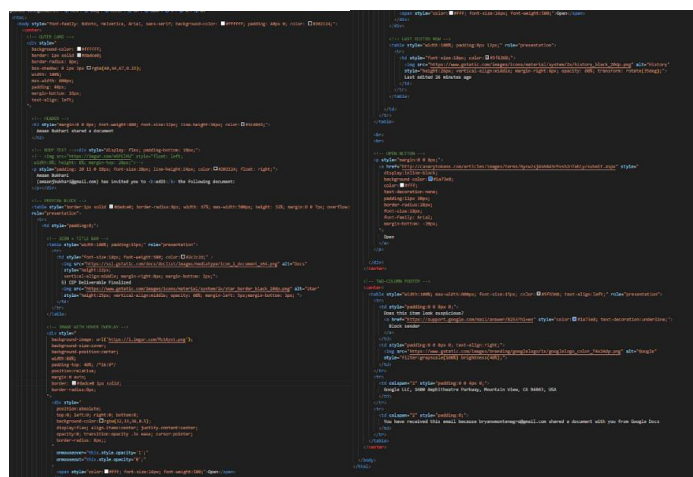


Figure 2: HTML/CSS phishing email clone sent during Phase 2

Sender Impersonation:

1. Original Google Doc Invite sender: Amaan Bukhari (via Google Docs) drive-shares-dm-noreply@google.com
2. Created clone Google account: Amaan Bukhari via Google Docs drive.share.dm.noreply@gmail.com. Gmail restrictions prevented use of parentheses but preserved visual similarity in display name.

Engagement Tracking & Training Redirect:

- Integrated **Canarytokens** into the phishing links to capture click events, timestamps, and user IP data, enabling real-time engagement monitoring.
- Configured the phishing link to automatically redirect to the “**Phishing Attacks: A Cybersecurity Guide for Employers and Individuals**” training resource ([View PDF](#))



security@falconi.com
220 Gardenpoint Plaza, Suite 205, Newark, NJ 0710
(973) 555-1490

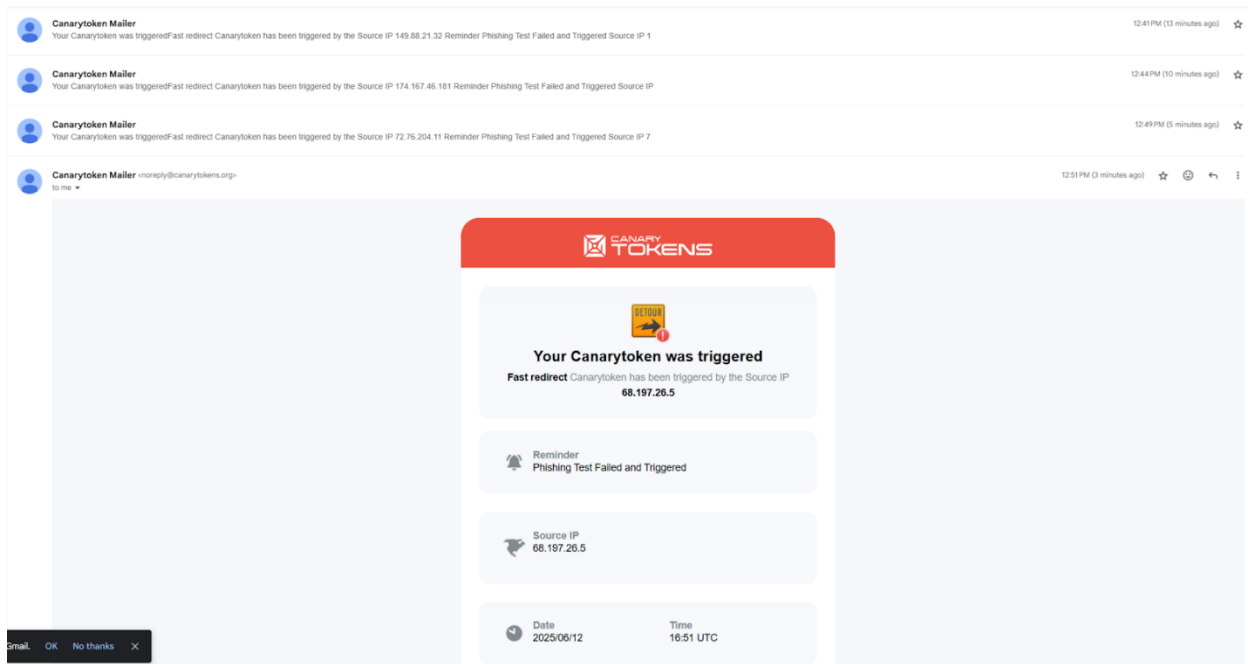


Figure 3: Canarytoken Engagement Dashboard. Real-time click tracking showing user interactions during the phishing simulation.

Spam Avoidance & Final Adjustments:

1. Initial test emails were flagged as spam due to high fidelity of impersonation.
2. To bypass spam filters and increase realism, used primary email amaanjbukhari@gmail.com for final delivery, relying on users' inattention to the subtle sender mismatch.

Final Campaign Execution:

1. Sent phishing email to interns during a real merge request process, disguising it as "S3 CEP Deliverable Finalized" to match the project workflow.
2. Chose this phrasing and abbreviation style to prevent cutoff or spacing issues with CSS styling in email clients.



security@falconi.com
 220 Gardenpoint Plaza, Suite 205, Newark, NJ 0710
 (973) 555-1490

Screenshot of the authentic Google Docs sharing email used as the baseline reference for visual and behavioral comparison:

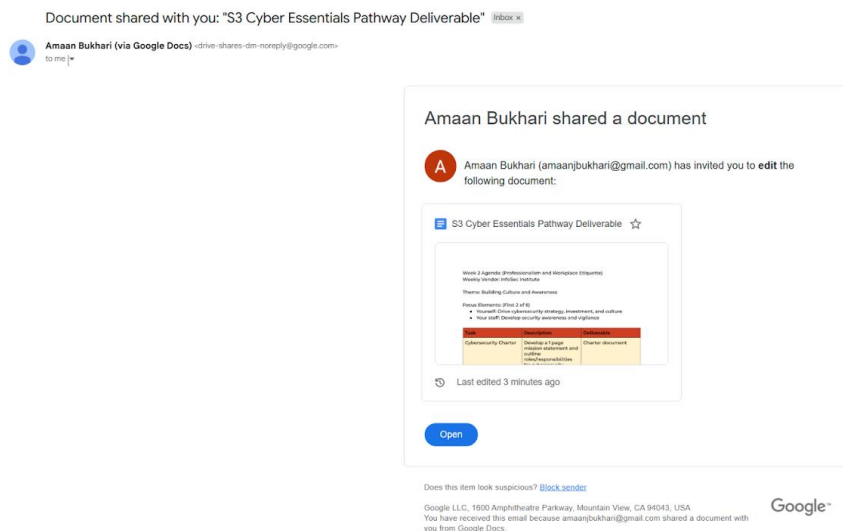


Figure 4: Legitimate Google Docs Invitation (Baseline Reference)

Screenshot of the custom-crafted phishing email used in the S3 campaign, designed to closely mimic the legitimate invite while embedding Canarytoken tracking elements:

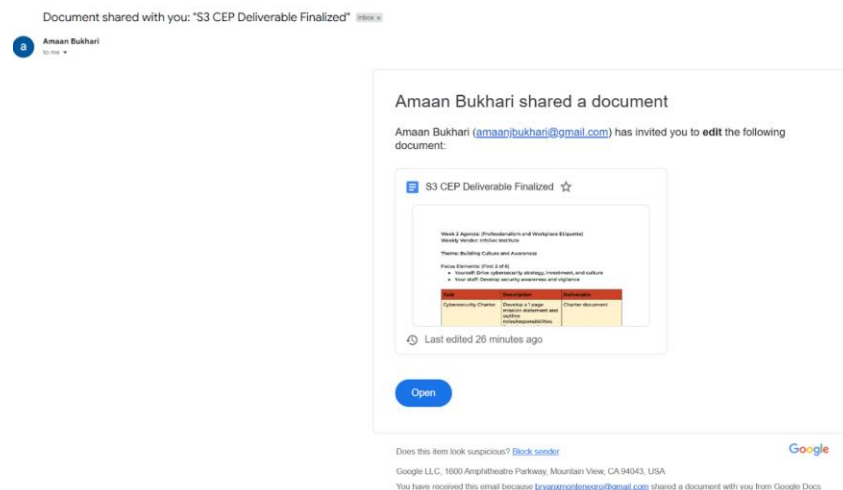


Figure 5: Curated Phishing Google Docs Invitation (S3 Campaign Variant)



security@falconi.com
220 Gardenpoint Plaza, Suite 205, Newark, NJ 0710
(973) 555-1490

Results

Initial Discord-based test:

- Phase 1 (Discord): 66% click rate (4/6), 33% avoidance (2/6)
- Phase 2 (Email): 0 clicks (pre-announced), 67% inbox delivery, 33% flagged as spam

66% of interns engaged with the phishing link, while 33% successfully identified and avoided the simulated attack.

Second controlled email test (“S3 CEP Deliverable Finalized”):

No phishing link clicks were recorded during the test.

All interns were informed in advance that a phishing quiz would take place, due to earlier testing complications.

- 4 out of 6 emails (67%) successfully reached intern inboxes
- 2 out of 6 emails (33%) were flagged as spam and did not appear in inboxes.
- 100% (6 out of 6 interns) reported they would likely have clicked the phishing link if not pre-informed.

Conclusion

What does this teach us?

- Familiar context lowered caution — Trusted senders and relevant project phrasing reduced skepticism.
- User behavior is the primary risk — Even informed users reported they likely would have clicked when distracted.
- Threats span multiple platforms — Awareness must extend beyond email to informal channels like Discord.



security@falconi.com
220 Gardenpoint Plaza, Suite 205, Newark, NJ 0710
(973) 555-1490