- Kyle Sershon
- CYSE368_24518
- Spring - 2026
- Teresa Duvall
- Joshua Russell
- The Global Electronics Association
- Reflection #1

Internship Reflection Journal 1

At The Global Electronics Association, I have worked on several tasks of the 1st 50 hours relating to our organization's security. The tasks I completed required extensive in-depth analysis of our internal network and systems. I worked mostly on remediation tasks related to penetration testing as we prepared for a retest. Additionally, I was responsible for creating a Security Awareness Training module for Newly Hired employees and a Phishing campaign to analyze how susceptible our employees were.

First, we reviewed the 84-page report and planned our remediation steps. I learned that there are many vulnerabilities that could be exploited; however, some carry more weight than others. I worked with my supervisor and team to remediate the high-risk threats. This gave me valuable insight into the annual penetration testing process and how it strengthens our defenses. The remediation process, which was required before retesting on 2/6/2026, required me to update the weak password policy and assist with other critical items. We strengthened our password policy to align with Synercomm's recommendations and industry standards. The penetration testing documentation gave me a clear view of the

issues in our environment and how an attacker could exploit each vulnerability. We worked on reviewing and implementing changes from 1/23/2026 to 2/5/2026.

Changes to the environment, such as password policy updates through Group Policy, affect not only IT but the entire organization, so careful planning and communication were required. Other changes required proper planning and documentation in case a rollback was needed due to disrupted business operations. We would then review the change and determine whether it represented an acceptable risk to the organization. I implemented the password policy changes in the local Active Directory on 2/2/2026. This also included a list of forbidden passwords, which included any domain or company names and terms.

In addition to Penetration testing remediation, I worked with KnowBe4 to create a Cyber Security Awareness Training Module for newly hired employees. This training is important because it will help mitigate the biggest weakness in any organization, the “Human Factor.” The training consisted of KnowBe4’s Annual 45-minute training video. In addition to creating this campaign, I used Knowbe4 to create a Simulated phishing campaign to help evaluate our organizational risk. The campaign took place between 2/4/2026 – 2/6/2026. The results of the camping exercise gave us insight into how susceptible our employees are to phishing attempts. It showed me that ongoing training is detrimental to an organization's security posture.

Conclusion

In conclusion, I found my hands-on involvement in Penetration testing remediation gave me an exclusive look into current vulnerabilities, how they can be exploited, and practical knowledge for resolving them. I understood the importance of documentation and communication to our staff regarding changes in organizational security standards. Using KnowBe4's platform was rewarding as well because it demonstrated the importance of annual training and the risks it can help mitigate.

Screenshots of Tasks :

Affected Systems or URLs

Remediated 0 of 1

☐ Domain password policy

Description & Impact

Any password policy requiring a length fewer than 14 characters or complexity fewer than 3 character types is considered weak. Policies that do not meet this requirement are likely to produce passwords that are easily guessed and/or cracked. When a weak password policy is in place, attackers will have a higher chance of success with various password spraying techniques. Password spraying is generally referred to as the practice of attempting logins on company systems with known usernames and commonly used passwords, such as Spring25, Password1234, and Welcome1.

Remediation & Mitigation Options

SynerComm recommends implementing a password policy that prevents users' passwords from being guessed and/or their password hash from being cracked. SynerComm recommends having at minimum the following characteristics for the password policy:

- Minimum 14 characters
- Password Complexity Enabled
- Last 10 passwords remembered
- Restriction of certain common words (seasons, football teams, the company name, "password" etc.)

Additionally, consider using Active Directory Fine Grained Password Policies for highly privileged accounts (Domain Admins, etc.). These policies can be associated to an Active Directory group of users. Requires Domain Functional Level 2008 or greater. Security controls such as Azure AD Password Protection may also be useful for blacklisting common base words used to create passwords.

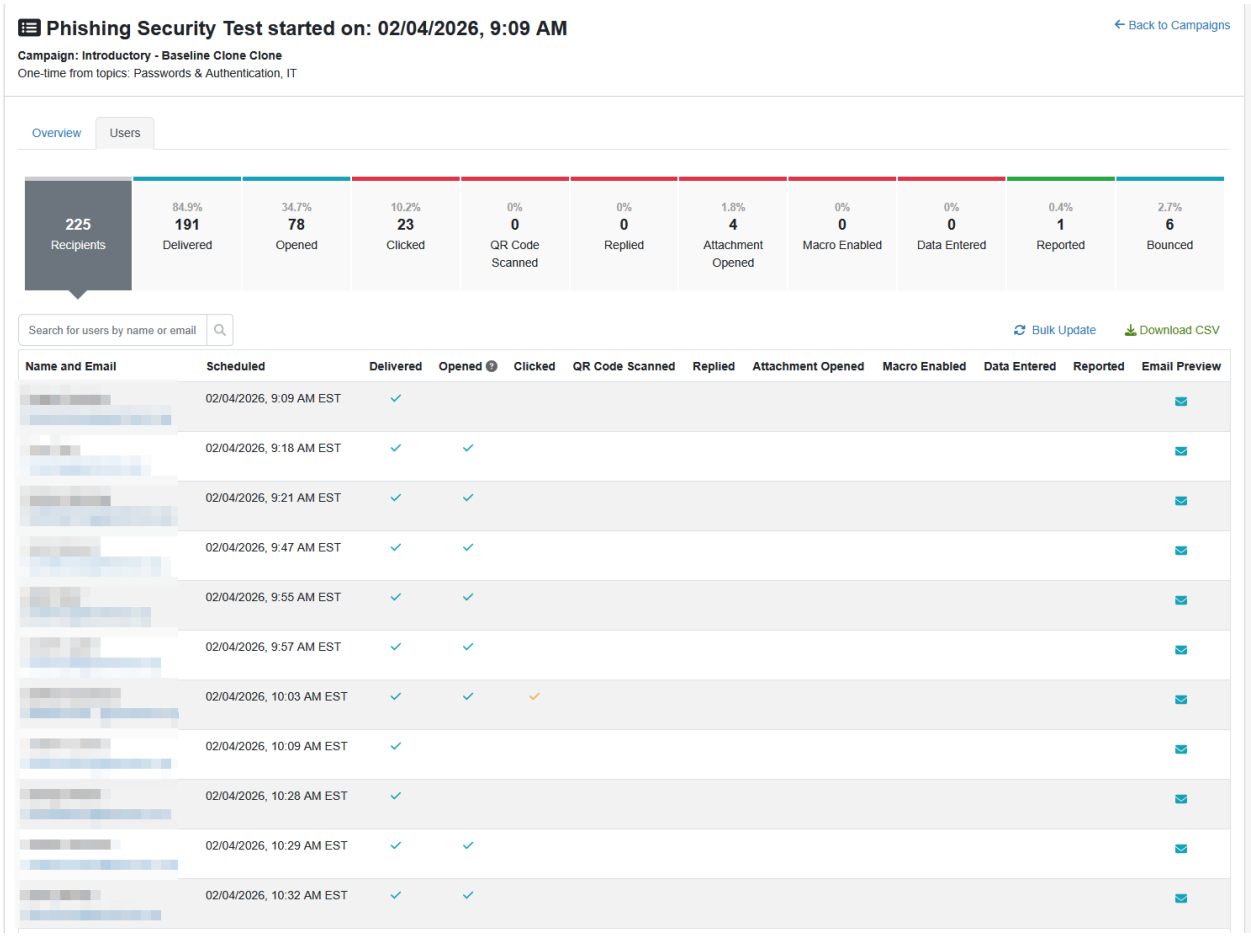
Disclaimer: While all SynerComm Findings and Recommendations are intended to remediate and mitigate risk, making changes comes with its own risk. This vulnerability and any proposed solutions should be appropriately researched and tested. Always follow your change control procedures.

References

SynerComm Blog - Why 14 characters?:
https://www.synercomm.com/blog/why-14-characters/

Active Directory Fine Grained Password Policies:
http://technet.microsoft.com/en-us/library/cc770394%28v=ws.10%29.aspx

Eliminate Bad Passwords Using Azure AD Password Protection:
https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-password-ban-bad


Phishing Security Test started on: 02/04/2026, 9:09 AM
Back to Campaigns
Campaign: Introductory - Baseline Clone Clone
One-time from topics: Passwords & Authentication, IT
Overview
Users
225 Recipients
84.9% 191 Delivered
34.7% 78 Opened
10.2% 23 Clicked
0% 0 QR Code Scanned
0% 0 Replied
1.8% 4 Attachment Opened
0% 0 Macro Enabled
0% 0 Data Entered
0.4% 1 Reported
2.7% 6 Bounced
Search for users by name or email
Bulk Update
Download CSV
Name and Email
Scheduled
Delivered
Opened
Clicked
QR Code Scanned
Replied
Attachment Opened
Macro Enabled
Data Entered
Reported
Email Preview
02/04/2026, 9:09 AM EST
02/04/2026, 9:18 AM EST
02/04/2026, 9:21 AM EST
02/04/2026, 9:47 AM EST
02/04/2026, 9:55 AM EST
02/04/2026, 9:57 AM EST
02/04/2026, 10:03 AM EST
02/04/2026, 10:09 AM EST
02/04/2026, 10:28 AM EST
02/04/2026, 10:29 AM EST
02/04/2026, 10:32 AM EST