NORTHWEST NAZARENE UNIVERSITY

First All-Company Annual Cybersecurity Training at Woodgrain

THESIS

Submitted to the Department of Mathematics and Computer Science

in partial fulfillment of the requirements

for the degree of

BACHELOR OF SCIENCE

Ender Sandidge

2023

THESIS

Submitted to the Department of Mathematics and Computer Science

in partial fulfillment of the requirements

for the degree of

BACHELOR OF SCIENCE

By

Ender Sandidge

2023

First All-Company Annual Cybersecurity Training at Woodgrain

Author: Ender Sandidge

Ender Sandidge

Approved: Barry Myers

Barry L. Myers, Ph.D., Chair, Department of Mathematics & Computer Science, Faculty Advisor

Approved:

Christa R. Sandidge, M Ed., Ed.D, Director, Center for Professional Development, Second Reader

Approved: Barry Myers

Barry L. Myers, Ph.D., Chair, Department of Mathematics & Computer Science

Abstract

First All-Company Annual Cybersecurity Training at Woodgrain Inc.

ENDER SANDIDGE (Department of Mathematics and Computer Science).

The project was completed throughout an internship at Woodgrain Inc. in their cybersecurity department. Responsibilities included designing, generating support for, and running Woodgrain's first annual cybersecurity training. This incorporated selecting the training modules, building the communication that would be sent out to employees, generating support with the lead team, and keeping other teammates up to date with the progress of the project. The responsibilities also entailed running the training itself, which involved creating the training in our education tool, answering questions from employees, and troubleshooting any problems that occurred throughout the process. Ultimately the training exceeded its goal of a seventy-five percent completion rate. Because of the success of this project the annual training has been expanded to also include new hires throughout the year. Additionally, the same format is being utilized to send out a security awareness proficiency assessment to gain better insight into how Woodgrain employees view cybersecurity. Finally, annual training will be continued each year, although the training modules will be changed for next year.

Acknowledgements

I would like to begin by thanking Terrance Paternoster, the director of cybersecurity at Woodgrain during the time of my project. He brought me onto the team and served as a mentor as I entered into the professional world of cybersecurity. I would also like to thank the organization of Woodgrain for giving me the opportunity to pursue this project and also allowing me to take creative control over how the training would play out. I would like to thank my professors, most notably, Dr. Myers and Dr. McCarty, for giving me the skills necessary to succeed in the position that I was placed in. I would not have had the success I did without their tutelage. Additionally, I am appreciative of the other students that have gone through the cybersecurity program here at Northwest Nazarene University with me. Finally I would like to thank my mother for the indescribable amount of support that she has given me, both in the form of consistent feedback regarding my work as I moved through college but also her unending encouragement.

Table of Contents

List of Figures

Overview

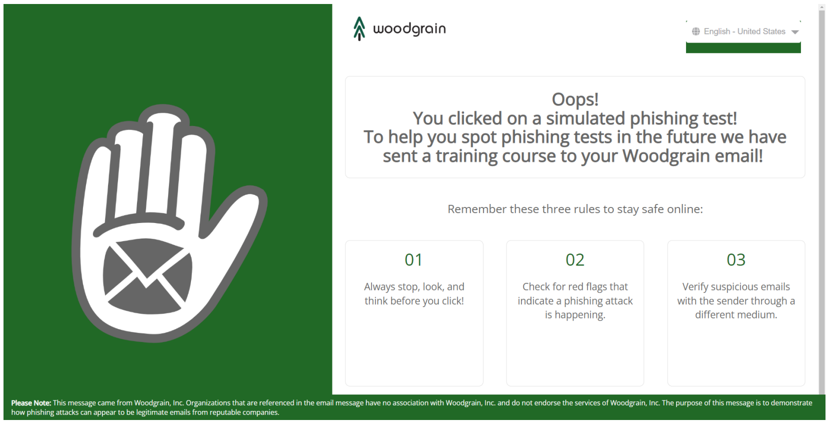
This project was designed with the purpose of planning, creating and conducting the first annual full company cybersecurity training at Woodgrain. The project was completed throughout the duration of an internship in the cybersecurity department at Woodgrain. The team which completed the project was composed of Ender Sandidge, Cyber Security Analyst Intern, and Terrance Paternoster, the Director of Cybersecurity at Woodgrain. The key aspects of this project included selecting the training modules, building the communication that would be sent out to employees, generating support with the lead team, and keeping other teammates up to date with the progress of the project. The responsibilities also entailed running the training itself, which involved creating the training in our education tool, answering questions from employees, and troubleshooting any problems that occurred throughout the process. An additional aspect of this project that can not be overlooked was preparing the culture of Woodgrain for the implementation of all-company mandatory cybersecurity training. This was accomplished through the administration of mandatory cybersecurity training for users who failed an automated phishing test and a weekly informative email about an aspect of cybersecurity sent to every employee. Each of these aspects were combined to encompass the totality of the senior project.

Background

Woodgrain is a privately held manufacturing company. There are around fifty sites spread all across the country with one additional site located in Chile. Additionally, there are around 2200 employees who work at Woodgrain with around 1200 of those actively utilizing their email accounts. To properly understand the challenges that came with the development of the all company cybersecurity training an individual needs to know the attitude towards cybersecurity held at Woodgrain. The cybersecurity department was started a year before the internships began in the spring of 2021. At the time the internship started, the only other employee within the cybersecurity department was Terrance Paternoster, the Director of Cybersecurity. He was building the program from the ground up which included many foundational pieces. Certain aspects that can be expected of a cybersecurity at a larger program were missing at Woodgrain when the internship began. There was no up to date policy regarding cybersecurity within the organization, and Woodgrain did not have an endpoint detection response (EDR) tool at the time the internshipship began. Due to the organization being privately owned these common expectations were not required by a governing body so the organization was left to make its own decisions regarding its need for cybersecurity. This was exacerbated by the fact that Woodgrain does very little direct to consumer sales so there was even less regulation due to a lack of held personally identifiable information (PII). One of the processes that was in place was automated phishing being conducted in order to measure the organization's ability to detect phishing attacks. The automated phishing was being conducted utilized the training platform KnowBe4, this is the platform that was used to send out the all company cybersecurity training. Because of all of these factors the organization was not prepared to jump right into all company cybersecurity training and a scaffolded approach was going to be needed, but some tools were in places that could be utilized to jumpstart that process.

Prior Cybersecurity Programs

In order to prepare the employees of Woodgrain for the implementation of an all-company mandatory cybersecurity training, two cybersecurity processes were begun. The first was mandatory training that was required for individuals who failed the automated phishing tests which were conducted weekly. The process began when a user clicked a bad link, the link would take them to a site where they would see the following landing page:



Oops!
You clicked on a simulated phishing test!
To help you spot phishing tests in the future we have sent a training course to your Woodgrain email!

Remember these three rules to stay safe online:

01
Always stop, look, and think before you click!

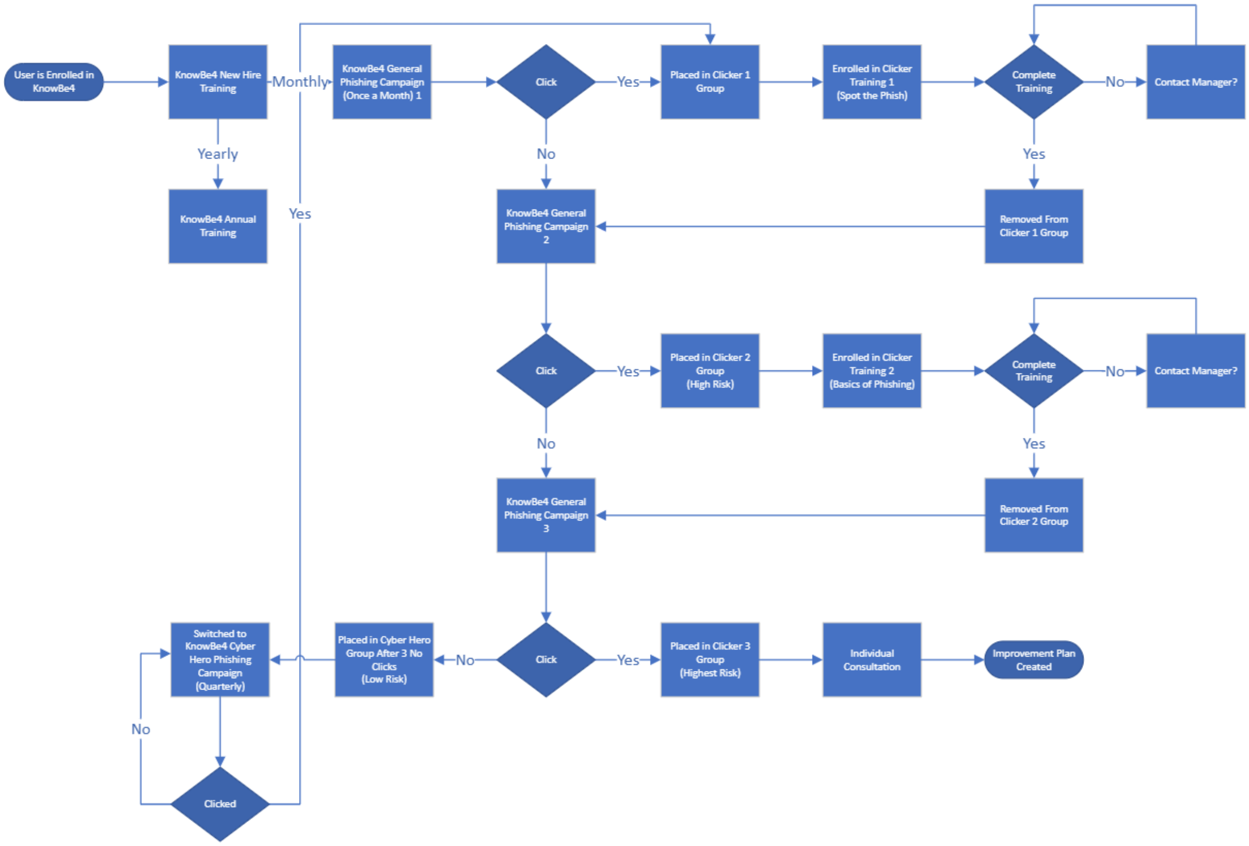
02
Check for red flags that indicate a phishing attack is happening.

03
Verify suspicious emails with the sender through a different medium.

Please Note: This message came from Woodgrain, Inc. Organizations that are referenced in the email message have no association with Woodgrain, Inc. and do not endorse the services of Woodgrain, Inc. The purpose of this message is to demonstrate how phishing attacks can appear to be legitimate emails from reputable companies.

Figure 1: Clicker Training Landing page

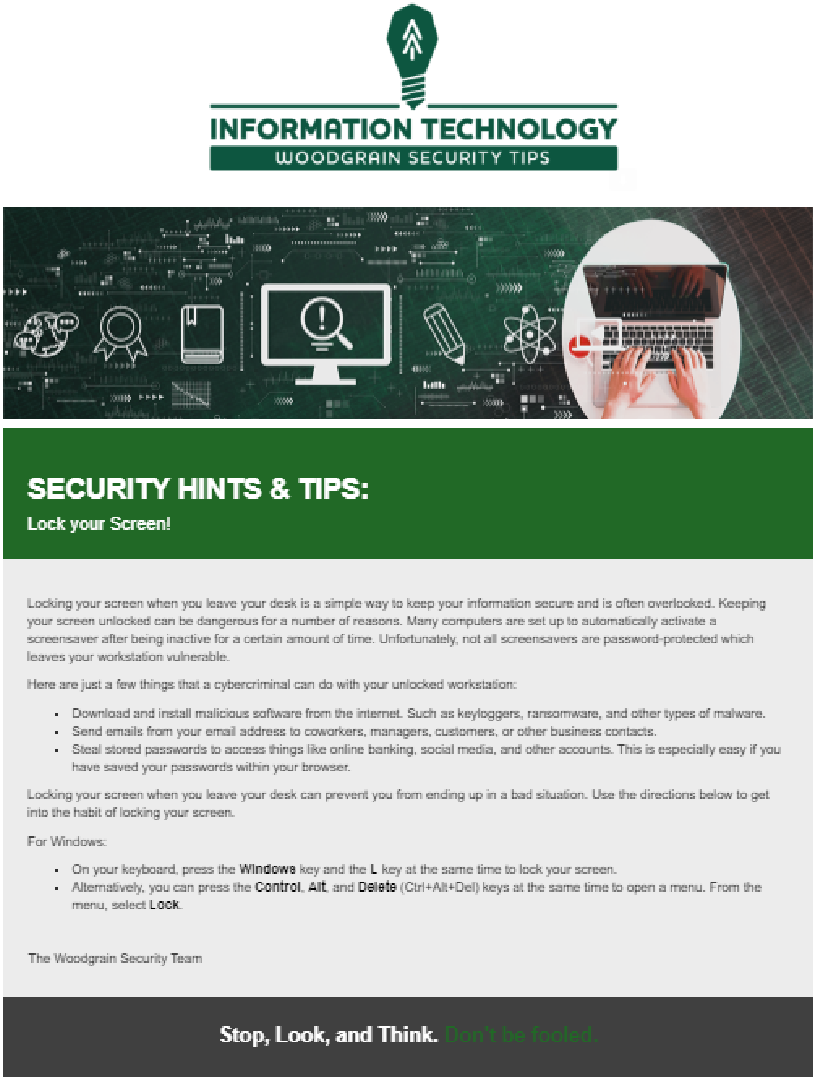
Then an automated process would happen on the backend of our training platform resulting in the users who had clicked on a phishing link being enrolled in a training program based on how many times they have clicked in the past. The process for how this training is assigned on the backend can be found in the flowchart diagram below:



User is Enrolled in KnowBe4
KnowBe4 New Hire Training
Monthly
KnowBe4 General Phishing Campaign (Once a Month) 1
Click
Yes
Placed in Clicker 1 Group
Enrolled in Clicker Training 1 (Spot the Phish)
Complete Training
No
Contact Manager?
Yearly
KnowBe4 Annual Training
Yes
No
Yes
KnowBe4 General Phishing Campaign 2
Removed From Clicker 1 Group
Click
Yes
Placed in Clicker 2 Group (High Risk)
Enrolled in Clicker Training 2 (Basics of Phishing)
Complete Training
No
Contact Manager?
No
Yes
KnowBe4 General Phishing Campaign 3
Removed From Clicker 2 Group
Switched to KnowBe4 Cyber Hero Phishing Campaign (Quarterly)
Placed in Cyber Hero Group After 3 No Clicks (Low Risk)
No
Click
Yes
Placed in Clicker 3 Group (Highest Risk)
Individual Consultation
Improvement Plan Created
No
Clicked

Figure 2: Flowchart Clicker Training

After they were assigned the training on the backend, they would receive an email with a link to the training that they had to complete. The other process that was started to get employees thinking about cybersecurity was a “Weekly Hints and Tips.” The Weekly Hint and Tip is an email that all employees would receive each week which contained some interesting information about cybersecurity. This served to keep cybersecurity in the forefront of employees’ minds and to make sure that they understood the importance of cybersecurity. An example of one of these “Weekly Hints and Tips” can be found in the figure below:



SECURITY HINTS & TIPS:

Lock your Screen!

Locking your screen when you leave your desk is a simple way to keep your information secure and is often overlooked. Keeping your screen unlocked can be dangerous for a number of reasons. Many computers are set up to automatically activate a screensaver after being inactive for a certain amount of time. Unfortunately, not all screensavers are password-protected which leaves your workstation vulnerable.

Here are just a few things that a cybercriminal can do with your unlocked workstation:

- Download and install malicious software from the internet. Such as keyloggers, ransomware, and other types of malware.
- Send emails from your email address to coworkers, managers, customers, or other business contacts.
- Steal stored passwords to access things like online banking, social media, and other accounts. This is especially easy if you have saved your passwords within your browser.

Locking your screen when you leave your desk can prevent you from ending up in a bad situation. Use the directions below to get into the habit of locking your screen.

For Windows:

- On your keyboard, press the **Windows** key and the **L** key at the same time to lock your screen.
- Alternatively, you can press the **Control**, **Alt**, and **Delete** (Ctrl+Alt+Del) keys at the same time to open a menu. From the menu, select **Lock**.

The Woodgrain Security Team

Stop, Look, and Think. Don't be fooled.

Figure 3: Weekly Hints and Tips Example

Pilot Training

The other piece of preparation that was conducted in advance of the implementation of the annual cybersecurity training was a pilot training with a small group of select employees. Employees, from a variety of departments at Woodgrain, were selected based on proven records of participation in cybersecurity related activities, for instance reporting test phishing emails.. Those users were enrolled in a training that included a much larger variety of training content then would be provided in the all company training. This pilot program served a couple of purposes. The first objective was to ensure that all of the software was working properly and as expected. Having a trial run with a smaller group of individuals made troubleshooting much easier and if anything had gone awry there would have been much fewer people that would need to be informed on what had not worked as intended. Secondly, by including a larger set of training modules, the team was able to choose the most effective trainings to present to the company as a whole. The team determined the most effective training by conducting a survey sent to all pilot trainees after they had completed all of their training. Included is a figure of each training module that was tested please see below:

Pilot Training		
Passwords	Phishing	Other
Creating Strong Passwords - Security Awareness Training	Phish or Treat? Phishing Edition	Micro-Module - Social Engineering
How to Create Strong Passwords with Quiz	10 Ways to Avoid Phishing Scams with Quiz	Micro-Module - Introduction to Ransomware
Cyber Heroes Series: Password Tips	Phishing Attacks on Companies with Quiz	Security Moment Series: Ransomware
	You are a Target!	Information Security @ Social Media
	Security Moment Series: Spot the Bad Attachment	Security Moment Series: Hacking Emotions

Figure 4: Pilot Training Modules

The training modules were divided into three separate categories in order to ensure that the most important topics were covered and that some variety was also achieved. The training in total added up to around 60 minutes of content. The final goal of the pilot training was to have a number of employees at a variety of sites that had already taken the training that could serve as resources for other employees. It can be easier for a user to reach out to another employee from a similar position or one that they see in person for help or guidance than to send an email to their cybersecurity department. Pilot training was another method that the team utilized in order to have a culture at Woodgrain that was more prepared for the annual cybersecurity training.

Annual Training Design

Following the completion of the pilot training the design of the actual annual training was set to begin. The first step was to narrow down the pilot training modules to the selections that would be used for the annual training. The team had decided on a training length of around 30 minutes so the amount of training from the pilot training would need to be cut in half. Using the results from our survey the team arrived at the following trainings to be sent out to the company at large:

Pilot Training		
Passwords	Phishing	Other
Creating Strong Passwords - Security Awareness Training	Phish or Treat? Phishing Edition	Micro-Module - Social Engineering
	Security Moment Series: Spot the Bad Attachment	Micro-Module - Introduction to Ransomware
		Security Moment Series: Hacking Emotions

Figure 5: Final Training Modules

The next step was to decide on a goal that the team would aspire to achieve in terms of completion rate. This was a process that all members of the Woodgrain security team participated in. After a discussion it was decided that our target completion rate would be

75% with a stretch goal of 85%. This was inline with the completion rate that was being seen with our mandatory clicker training; the completion rate was around 70% at the time. After the goal completion rate was determined the next step was to decide on which users would be required to take the training. While in an ideal world since it is an all company training it would be sent to the entire organization this is not possible at Woodgrain for a few reasons. As a manufacturing organization there are many employees who work the shop room floor and never access a computer. These individuals may have Woodgrain email accounts but very rarely, if ever log into them. This makes cybersecurity training unnecessary for them. Additionally, there was a significant possibility that they would not complete the training and lower our completion rate. As a cybersecurity department it was decided that the target audience was all employees who had logged into their email accounts within the last two months to be required to take the training. To complete this goal a query was run that put the relevant data into a csv. which was then imported into KnowBe4, our training platform. Finally, there was a need to determine the training timeline. It was decided to conduct the training for one month to ensure employees would have ample time to complete the training without it affecting their day to day responsibilities. Additionally, the training was divided into a series of modules that could be completed individually. Having the training be broken up into multiple modules aligned with the idea of offering the training over a longer period of time. This resulted in us building out the following timeline for the dates that the training would be offered:

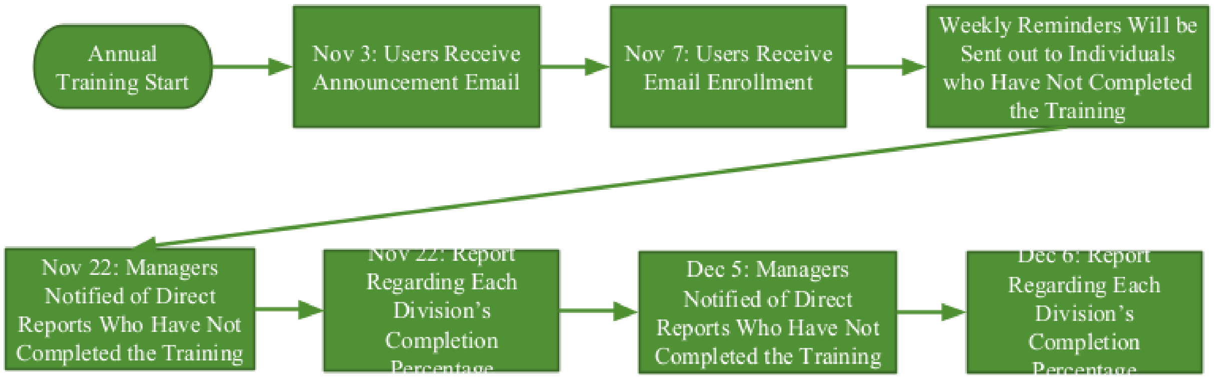
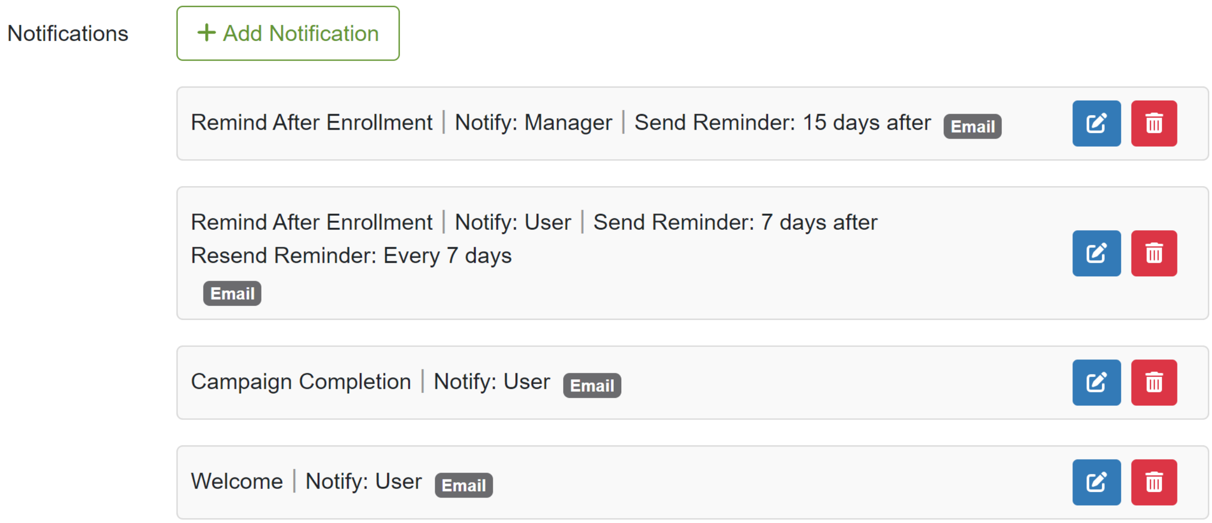

Annual Training Start
Nov 3: Users Receive Announcement Email
Nov 7: Users Receive Email Enrollment
Weekly Reminders Will be Sent out to Individuals who Have Not Completed the Training
Nov 22: Managers Notified of Direct Reports Who Have Not Completed the Training
Nov 22: Report Regarding Each Division's Completion Percentage
Dec 5: Managers Notified of Direct Reports Who Have Not Completed the Training
Dec 6: Report Regarding Each Division's Completion Percentage

Figure 6: Annual Training Timeline

After the final decisions on each of those aspects of how the training would look were made, the training plan was presented to the Woodgrain Leadership Team to gain approval for the specifics of the training and to ask for their support as the organization went forward with the training. This was done with the utilization of a powerpoint presentation during one of their all lead team meetings. Following this presentation the go ahead was granted and the training began using the timeline outlined in figure 6.

Annual Training Notifications

The final aspect of the annual training was the notifications that would be sent out to each of the employees taking the training to remind them to complete it if they have not already done so. The sending of these reminders was automated through the use of our training platform, with two exceptions; the first initial announcement email was not sent through the platform and periodic updates to the lead team regarding the status of the training did not go out through the training platform. The schedule of the notifications that were sent through the training platform can be seen in the following figure:



Remind After Enrollment | Notify: Manager | Send Reminder: 15 days after Email

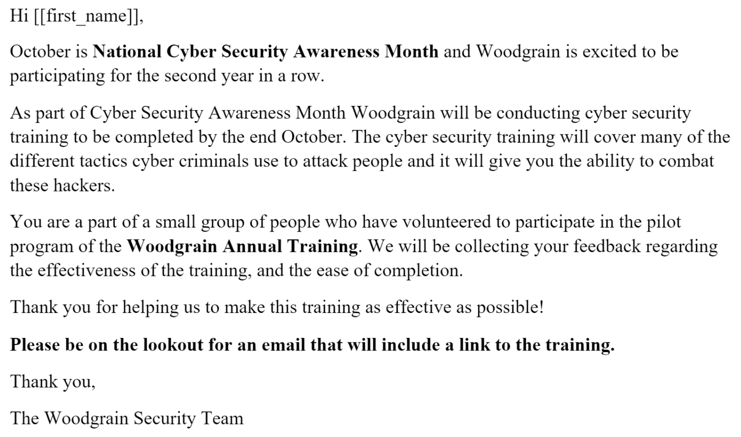
Remind After Enrollment | Notify: User | Send Reminder: 7 days after
Resend Reminder: Every 7 days
Email

Campaign Completion | Notify: User Email

Welcome | Notify: User Email

Figure 7: All Notifications

Here are each of the emails that we used KnowBe4 to send out automatically. At the top of figure 7 you can see the enrollment email which includes the link to the training. This is not the first email notification that was sent out about the training, A notification was sent out previously letting employees know about the training which did not include a link. It is essential these two emails are split up because you do not want employees to be clicking on random links that show up in their inbox so the employees were prepped with an announcement email in advance. The first email that was sent which did not include a link can be seen below:



Hi [[first_name]],

October is **National Cyber Security Awareness Month** and Woodgrain is excited to be participating for the second year in a row.

As part of Cyber Security Awareness Month Woodgrain will be conducting cyber security training to be completed by the end October. The cyber security training will cover many of the different tactics cyber criminals use to attack people and it will give you the ability to combat these hackers.

You are a part of a small group of people who have volunteered to participate in the pilot program of the **Woodgrain Annual Training**. We will be collecting your feedback regarding the effectiveness of the training, and the ease of completion.

Thank you for helping us to make this training as effective as possible!

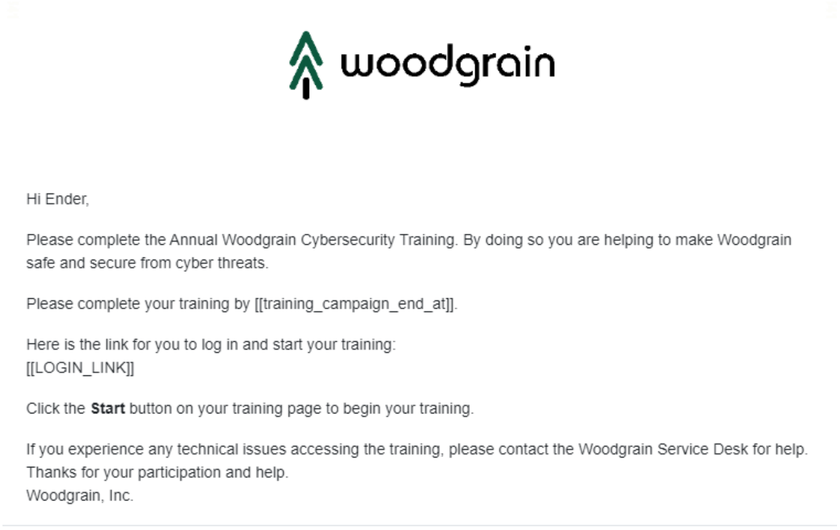
Please be on the lookout for an email that will include a link to the training.

Thank you,

The Woodgrain Security Team

Figure 8: Announcement Email

Following the announcement email the enrollment email was sent out which included the link to the training. This email can be seen below:



woodgrain

Hi Ender,

Please complete the Annual Woodgrain Cybersecurity Training. By doing so you are helping to make Woodgrain safe and secure from cyber threats.

Please complete your training by [[training_campaign_end_at]].

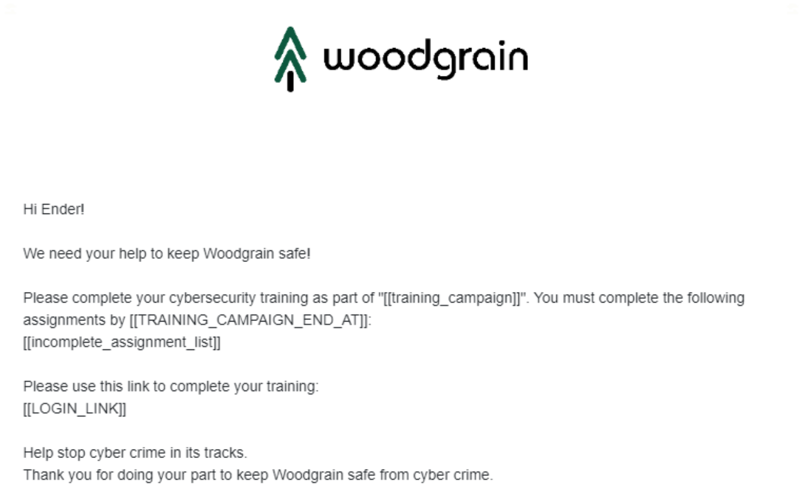
Here is the link for you to log in and start your training:
[[LOGIN_LINK]]

Click the **Start** button on your training page to begin your training.

If you experience any technical issues accessing the training, please contact the Woodgrain Service Desk for help.
Thanks for your participation and help.
Woodgrain, Inc.

Figure 9: Enrollment Email

In order to make sure that employees did not forget about the training, weekly reminders were sent. An example of this email can be seen below:



woodgrain

Hi Ender!

We need your help to keep Woodgrain safe!

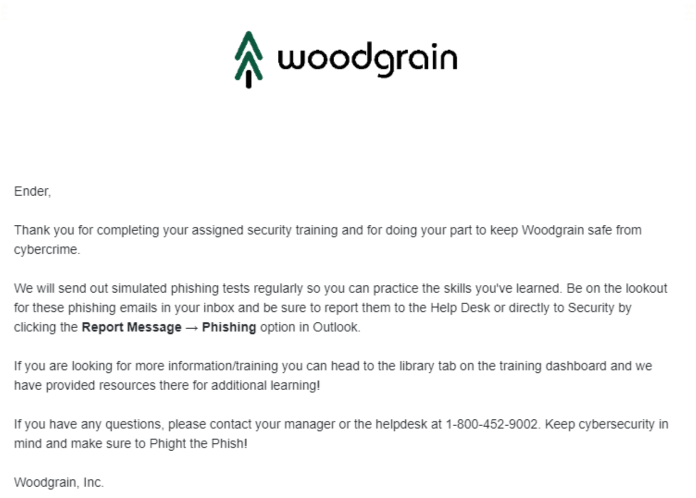
Please complete your cybersecurity training as part of "[[training_campaign]]". You must complete the following assignments by [[TRAINING_CAMPAIGN_END_AT]]:
[[incomplete_assignment_list]]

Please use this link to complete your training:
[[LOGIN_LINK]]

Help stop cyber crime in its tracks.
Thank you for doing your part to keep Woodgrain safe from cyber crime.

Figure 10: Weekly Reminder Email

These weekly reminder emails would not be sent if the user completed the training. Following the completion of the training by the user they would receive the following email:



Ender,

Thank you for completing your assigned security training and for doing your part to keep Woodgrain safe from cybercrime.

We will send out simulated phishing tests regularly so you can practice the skills you've learned. Be on the lookout for these phishing emails in your inbox and be sure to report them to the Help Desk or directly to Security by clicking the **Report Message → Phishing** option in Outlook.

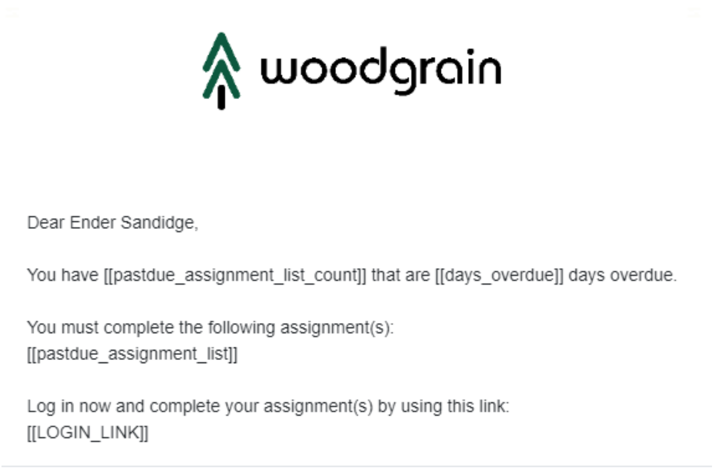
If you are looking for more information/training you can head to the library tab on the training dashboard and we have provided resources there for additional learning!

If you have any questions, please contact your manager or the helpdesk at 1-800-452-9002. Keep cybersecurity in mind and make sure to Phight the Phish!

Woodgrain, Inc.

Figure 11: Completion Email

This completion email provided positive reinforcement for users that completed the training and also put a stop to the weekly reminder emails. Both of these features would incentivize users to complete the training as quickly as possible. The next email that would be sent out if the user failed to complete the training within the allotted time was a past due reminder email. The training was left open to be completed after the set end date because it was anticipated that a large number of users would not complete the training until the deadline had passed, and this was planned upon. That email can be seen below:



Dear Ender Sandidge,

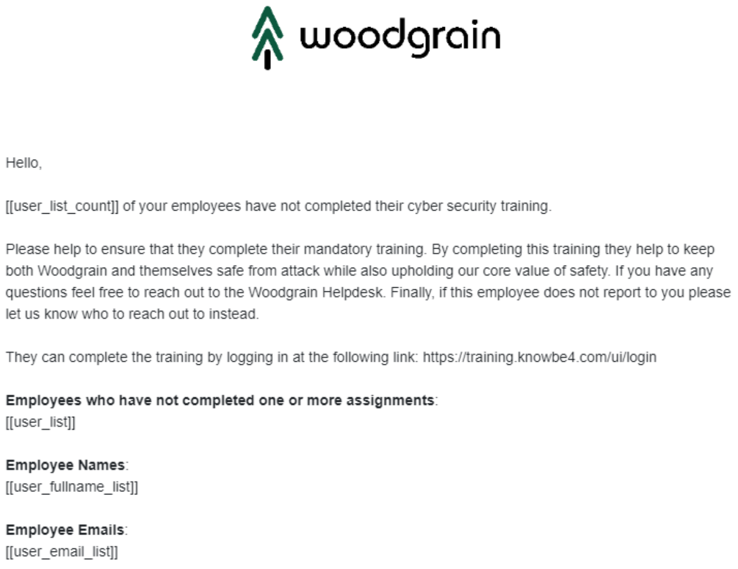
You have [[pastdue_assignment_list_count]] that are [[days_overdue]] days overdue.

You must complete the following assignment(s):
[[pastdue_assignment_list]]

Log in now and complete your assignment(s) by using this link:
[[LOGIN_LINK]]

Figure 12: Past Due Users

The direct managers of those users who had not completed the training were emailed and informed of their direct report’s failure to complete the training. The manager email was also sent at the halfway point of the training in order to incentivize the managers to encourage their employees to complete the training. This email can also be viewed below:



Hello,

[[user_list_count]] of your employees have not completed their cyber security training.

Please help to ensure that they complete their mandatory training. By completing this training they help to keep both Woodgrain and themselves safe from attack while also upholding our core value of safety. If you have any questions feel free to reach out to the Woodgrain Helpdesk. Finally, if this employee does not report to you please let us know who to reach out to instead.

They can complete the training by logging in at the following link: https://training.knowbe4.com/ui/login

Employees who have not completed one or more assignments:
[[user_list]]

Employee Names:
[[user_fullname_list]]

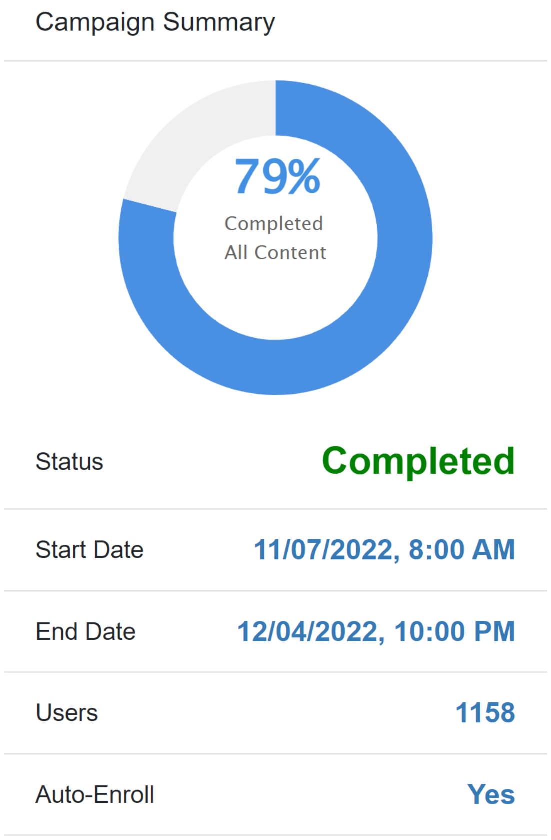
Employee Emails:
[[user_email_list]]

Figure 13: Past Due Managers

The only other communication that was sent out throughout this process were updates to the lead team regarding the progress of the organization in completing the training. This information was divided up so that the percentage completion rates were sorted by division.

Results

After the month had passed and the training had been completed, the training was kept open for one additional week. This allowed employees who had procrastinated until the very end an opportunity to complete the training. After everything was said and done the training had reached a completion rate of 79%. This exceeded our goal of 75% but did not reach our stretch goal. A campaign summary taken from our training portal can be seen below:

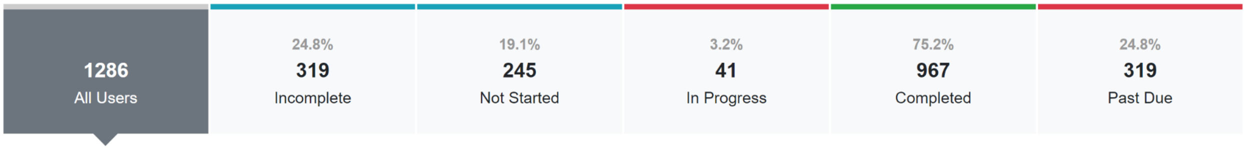


Campaign Summary

Status	Completed
Start Date	11/07/2022, 8:00 AM
End Date	12/04/2022, 10:00 PM
Users	1158
Auto-Enroll	Yes

Figure 14: Campaign Summary

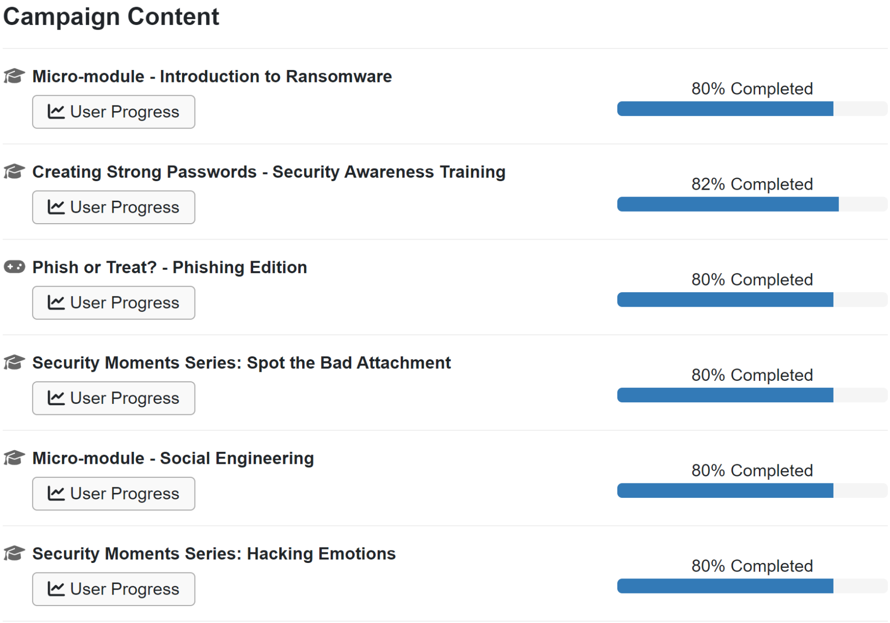
The breakdown of the number of users at each point of progress within the campaign provides additional insight into how our users performed. The figure can be seen below:



	24.8%	19.1%	3.2%	75.2%	24.8%
1286	319	245	41	967	319
All Users	Incomplete	Not Started	In Progress	Completed	Past Due

Figure 15: Campaign Breakdown

The 79% completion rate comes from users who completed each portion of the campaign but there is also a breakdown of completion rates by module which can be seen below:



Campaign Content

Module	Completion
Micro-module - Introduction to Ransomware User Progress	80% Completed
Creating Strong Passwords - Security Awareness Training User Progress	82% Completed
Phish or Treat? - Phishing Edition User Progress	80% Completed
Security Moments Series: Spot the Bad Attachment User Progress	80% Completed
Micro-module - Social Engineering User Progress	80% Completed
Security Moments Series: Hacking Emotions User Progress	80% Completed

Figure 16: Breakdown by Module

Additionally, graphs were created of the number of users that completed the training by date so that insight could be gained about what communications were most effective to get users to complete the training. This graph can be viewed below; it is set up with dates on the bottom and the number of users who completed the training on the left.

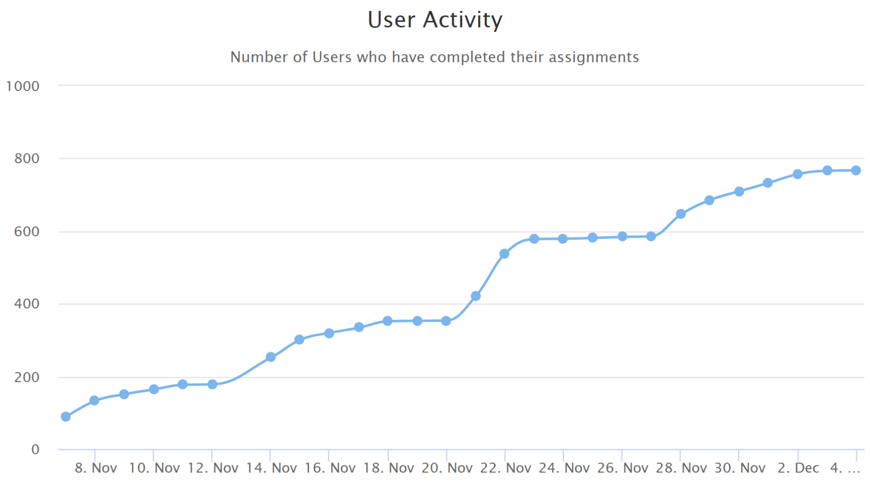
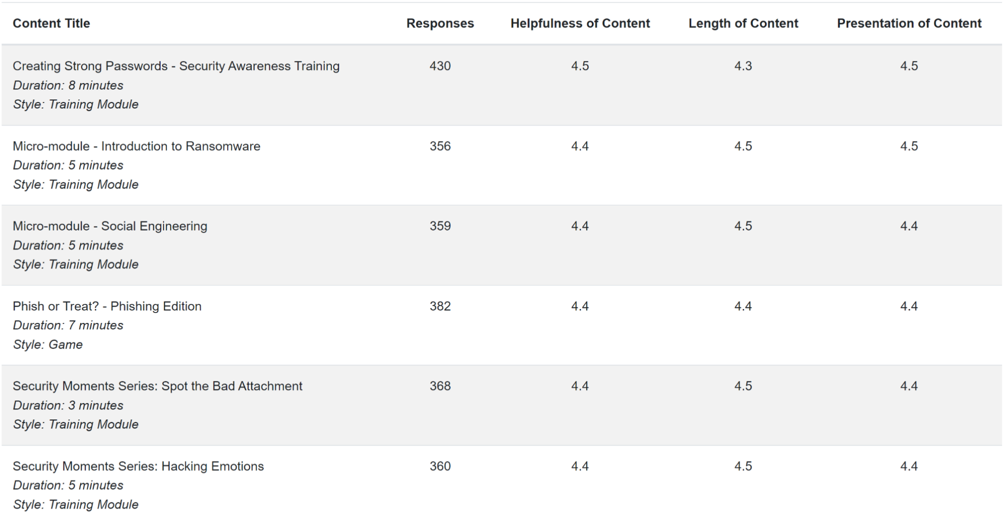


Figure 17: Users Completion Graph

As indicated on the graph, the largest spike was around the halfway point. This corresponds to the email being sent to managers about employees who have not completed the training. This data incentivized us to keep that notification in all of our campaigns moving forward. The final important piece of information that was gathered was through participant surveys. These surveys were conducted in each of the training modules that were used throughout the campaign. This will help us determine which training modules to use again in later years and which modules to avoid. See below for a breakdown of that data:



Content Title	Responses	Helpfulness of Content	Length of Content	Presentation of Content
Creating Strong Passwords - Security Awareness Training *Duration: 8 minutes* *Style: Training Module*	430	4.5	4.3	4.5
Micro-module - Introduction to Ransomware *Duration: 5 minutes* *Style: Training Module*	356	4.4	4.5	4.5
Micro-module - Social Engineering *Duration: 5 minutes* *Style: Training Module*	359	4.4	4.5	4.4
Phish or Treat? - Phishing Edition *Duration: 7 minutes* *Style: Game*	382	4.4	4.4	4.4
Security Moments Series: Spot the Bad Attachment *Duration: 3 minutes* *Style: Training Module*	368	4.4	4.5	4.4
Security Moments Series: Hacking Emotions *Duration: 5 minutes* *Style: Training Module*	360	4.4	4.5	4.4

Figure 18: User Surveys

As indicated in Figure 18, the data is comparable across the board; these results led us to believe that users were not putting much effort into their answers. Although unsurprising, the responses were disappointing because there was hope to gain further insight into what training should be utilized in the future.

Future Work

There are a few aspects of this project that have been taken forward and implemented into future projects and there are further plans as well. From this initial organizational wide training initiative, there is already implemented a new user training which is in the same format with the same training modules. New user training is currently in a pilot phase with only corporate being included. Moving forward the plan is to roll it out to the corporation at large within the next quarter. A similar training format to the all-company training is going to be utilized to send out a Security Awareness Proficiency Assessment. The Security Awareness Proficiency Assessment will help us know how knowledgeable our employees are about various aspects of cyber security. Finally, there will be continuing annual training each year following the same format with different training modules.

Conclusion

Working on this project was an incredible opportunity for me personally. It gave me the ability to take charge of my own project and see it through to the end. I was able to have oversight into each piece of the process and make the decisions that I thought would be the most beneficial. It gave me insight into what is expected of a security analyst within the workforce. I hope to take the experience I gained throughout this process forward as I move into the workforce.

I appreciated the support that I was provided with throughout each step of the process. Although I was given a lot of autonomy, if I was ever stuck or not sure how best to proceed, I was granted ample resources in order to ask questions and to receive advice. I never felt like I was put in a position where I would fail.

Finally, I was appreciative of the fact that the work I did was not only beneficial to my organization, but it will continue to provide a positive impact for years to come. The format for the training that I built will be used for all of our training moving forward, with plans already in place for additional training. Much of the work I did was automated so that it will be able to continue to positively impact the security landscape of Woodgrain as the organization moves forward.