Web Compromise

## Date: 2025-02-13

## Handler: Kush Patel

# Executive Summary

On 2025-02-12 at 10:00AM PST the Security Department notified the SOC about unusual behavior on one of their servers, the servers on the SecureTech company. The user smorgan@securetech.com reported that there was a phishing link sent by another internal user in the SecureTech which was [jrobinson@securetech.com](mailto:jrobinson@securetech.com), but we know that one of our users would never send a malicious phishing message like which indicates that his account was a victim of a cyber attack which was a compromised user account. The malicious website was “https://srv-61.kim.johnson.biz/login”, which was the same link sent to not just the one user who reported that incident but also other users who got the email, other users either ignored that message or clicked that link and entered and gave information to the website. On 2025 02-07 the users consistently sent out that email to other internal users in the securetech company, many users either ignored it, just opened it, or gave information which will probably cause them to loose information, their accounts to be compromised or more malicious things to happen to their accounts as well. The other internal users didn’t just receive that email with that link from [jrobinson@securetech.com](mailto:jrobinson@securetech.com) but other external email addresses that were infected, affected, or compromised by that web link because like [jrobinson@securetech.com](mailto:jrobinson@securetech.com) they also could’ve gave that link information which caused their accounts to be compromised and the attackers could’ve used this company as a target by using a internal user account along with external user account to avoid being caught. The user whos account was compromoised was able to still log in with his credentials and do his normal activities, which showed that his credentials weren’t modified but other data in his account was modified and hes at risk of getting in trouble and his reputation ruined because of his account being compromised Incident response measures we took were that we looked for any unauthorized logins or changes to the internal users, changed the credentials of the users, added data backups to the users, added a firewall so it would restrict traffic to that website, adding anti virus scanners to every account, implementing a security audit, more security controls, company wide shutdown of the servers, made mandatory credential changes to all users. We need to add multi factor aunthetication to all the servers on the company. Permantely kicking out [jrobinson@securetech.com](mailto:jrobinson@securetech.com) from the company. The financial impact of the incident includes developer labor, it specialist labor, investigative labor, and costs for implementing new technologies,

# Background

On Febuary 12 , 2025 , the security team of SecureTech was notified by a internal user who was [smorgan@securetech.com](mailto:smorgan@securetech.com), she informed the company that she received a phishing email from another internal user, the SOC then investigated the cyber attack which was an account compromise of an internal user which was jrobinson@securetech.com, which was caused when [jrobinson@securetech.com](mailto:jrobinson@securetech.com) went to the malicious website that was the phishing link which was “https://srv-61.kim.johnson.biz/login”, gave his information at that website based on the POST method shown in the http logs that showed his IP address. He received that email from an email called carrie64@ford.com from IP Address 23.74.164.69 which included that phishing link as part of his usual emails, after he sent his information, the attacker who most likely owned that website used his information to gain access to his securetech account, and once that attacker gained accessed to [jrobinson@securetech.com](mailto:jrobinson@securetech.com) he then found some documents and other email addresses of other internal users in the company, he then decided not to send that scam phshing link all under a single securetech account of when [jrobinson@securetech.com](mailto:jrobinson@securetech.com), he decided also use email addresses of other compromised email to send the malicious phishing link to the internal securetech users but he mostly sent those malicious links and messages with the compromised account of [jrobinson@securetech.com](mailto:jrobinson@securetech.com), the users who received that phishing link and opened that phishing link and then gave them their information. Based on the other POST methods at the websute <https://srv-61.kim.johnson.biz/login>, it showed that [sritter@securetech.com](mailto:sritter@securetech.com), [jfoster@securetech.com](mailto:jfoster@securetech.com), [bbarron@securetech.com](mailto:bbarron@securetech.com), [pmccoy@securetech.com](mailto:pmccoy@securetech.com),  [jball@securetech.com](mailto:jball@securetech.com), [mbutler@securetech.com](mailto:mbutler@securetech.com), all the secure tech users who gave their personal or any information to that phishing link, which will also cause their accounts to be compromised as well in the future, as well as loosing other potential and valuable information, we don’t know how the attacker compromised the accounts, but the information the accounts who gave their information based on the POST method indicates that the attacker used the information as a hint to find any valuable sensitive, or confidential information regardhing their accounts. The attacker did a lateral phishing in which the attacker sent the malicious employes to other internal employees within the company, the attacker who used mostly [jrobinson@securetech.com](mailto:jrobinson@securetech.com) along with other compromised emails spammed the other internal employee users in the company by sending them an email all at once, the attacker used [jrobinson@securetech.com](mailto:jrobinson@securetech.com) to find other secure tech users in the company, the compromised account of [jrobinson@securetech.com](mailto:jrobinson@securetech.com) received the usual emails like most the other users did and that malicious email was part of the usual emails that [jrobinson@securetech.com](mailto:jrobinson@securetech.com) received and he didn’t know that it was malicious, there were many users who opened the malicious link but didn’t give any information to that link but we should check their accounts just in case. The website was located at ip address 23.74.164.69, [jrobinson@securetech.com](mailto:jrobinson@securetech.com) was the only email in the securetech domain to send out an email while the other users in the securetech domain didn’t send out any emails and the mail logs showed that no other securetech user sent out any mails after the [jrobinson@securetech.com](mailto:jrobinson@securetech.com) was compromised. The other users and the compromised account of the [jrobinson@securetech.com](mailto:jrobinson@securetech.com) then received their usual emails like they did before the account was compromised. The attacker decided not to change credentials because he wanted to cover himself up and was trying to frame [jrobinson@secure.tech.com](mailto:jrobinson@secure.tech.com) but failed because we found out that the account was compromised. Some of the other users who gave the website their information may have their account sbeen compromised but they didn’t send it to other securetech users they instead did some other malicious activity like adding malicious plug ins with malware in it on other websites. The malicious website of   
srv-61.kim.johnson.biz” contained a log in page in which the user [jrobinson@securetech.com](mailto:jrobinson@securetech.com) logged into its credentials and the attacker gots all of its information and credentials and logged in to the website and because of this he sent out so many emails with [jrobinson@securetech.com](mailto:jrobinson@securetech.com) along with other compromised external emails outside the securetech domain and one of the internal users reported it when she opened the email..the company had to shut down all servers for investigation.

# Timeline

2025-02-06 at 9:08PM– [jrobinson@securetech.com](mailto:jrobinson@securetech.com) received an email from [carrie64@ford.com](mailto:carrie64@ford.com) l that contained the malicious link of “srv-61.kim.johnson.biz”, he then gave that website some credentials and information which then caused his account to be compromised by the attacker

2025-02-07 at 2:00AM to 2:10AM PST – the attacker logged into his secure tech account of – [jrobinson@securetech.com](mailto:jrobinson@securetech.com) ,compromised the account and sent that malicious phishing link of “srv-61.kim.johnson.biz”, to other internal securetech accounts within the company

2025-02-08 to 2025-02-12 – Other users in the company who reicieved that malicious link either opened that link and gave their information or just ignored that message which showed that other users in the company was at risk of having their data being stolen or accounts being compromised

2025-02-08 to 2025-02-12 –We discovered that [jrobinson@securetech.com](mailto:jrobinson@securetech.com) received and open some emails but didn’t do anything malicous on those emails which incidates that he wasn’t logged in as the attacker and his credentials like his password didn’t change

2025-02-12 at 12:00 PM PST – The user [smorgan@securetech.com](mailto:smorgan@securetech.com) reported the phishing email link to the security department of the company, the security department ordered a shutdown of all the servers and mandated all users to change their credentials

2025-02-13 at 10:00AM PST – The security department notified SOC of the incidient and the SOC began its investigation of what happend

2025-02-13 at 10:17AM PST – We discovered that Based on the Users IP address of 10.10.1.7, the user whos account was [jrobinson@securetech.com](mailto:jrobinson@securetech.com) opened the external link and gave his credentials to that external link

2025-02-13 at 10:22AM PST – We discovered that the user whos account was compromised sent out those emails containing the malicious link to other internal securetech users within the company which incidates he was trying to do a lateral phishing attack

2025-02-13 at 10:35AM PST – We discovered that the emails from [jrobinson@securetech.com](mailto:jrobinson@securetech.com) containing that malicious link came from the ip address of 23.74.164.69, which showed that an outsider compromised his email

2025-02-13 at 10:38AM PST –we discovered that [jrobinson@securetech.com](mailto:jrobinson@securetech.com) received an email from other outside emails both before and after his account was compromised and the attack was made which incidates that the aattacker didn’t change his credentials and jrobinson@securetech.com was still able to do his usual activites and was doing his other usual activities

2025-02-13 at 10:41AM PST –we discovered that [jrobinson@securetech.com](mailto:jrobinson@securetech.com) was the only secure tech user who sent out an email to other people all of which were other securetech employees, which showed that he was targeting other users in a phishing attack

2025-02-13 at 10:53AM PST –we discovered that users [sritter@securetech.com](mailto:sritter@securetech.com), [jfoster@securetech.com](mailto:jfoster@securetech.com), [bbarron@securetech.com](mailto:bbarron@securetech.com), [pmccoy@securetech.com](mailto:pmccoy@securetech.com), [jball@securetech.com](mailto:jball@securetech.com), and [mbutler@securetech.com](mailto:mbutler@securetech.com) received the phishing email opened the link logged in the website, and gave them information and credentials which caused the attacker to see their information and account information which would cause their accounts to be compromised as well

2025-02-13 at 10:55AM PST –We discovered that [jrobinson@securetech.com](mailto:jrobinson@securetech.com) sent out those phshing emails to the other internal users on Febuary 7th from 2:06 PM to 2:10 PM

2025-02-13 at 11:16AM PST –We discovered that [jrobinson@securetech.com](mailto:jrobinson@securetech.com) sent out those phshing emails to the other internal users on Febuary 7th from 2:06 PM to 2:10 PM

2025-02-13 at 11:21AM PST –We discovered that before [jrobinson@securetech.com](mailto:jrobinson@securetech.com) sent out those phshing emails he opened the malicious link way before he sent out those emails and everyone else who reiceved those emails opened it together in or around the same time frame.

2025-02-13 at 11:45AM PST –We discovered that the malicious website of “https://srv-61.kim.johnson.biz/login”, was owened by the attacker who compromised [jrobinson@securetech.com](mailto:jrobinson@securetech.com), which showed the company lacks scanning websites and url to determine if they are safe or secure

2025-02-13 at 2:45PM PST – We discovered that [jfoster@securetech.com](mailto:jfoster@securetech.com) was the first user to give the malicious website sent by the compromised account

2025-02-13 at 3:10PM PST – We discovered that [bbarron@securetech.com](mailto:bbarron@securetech.com) was the second user to open that malicious website and give them information, his account was compromised because he accessed a website and added a new thing which was malicious to the website

2025-02-13 at 3:40PM PST –We discovered that [pmccoy@securetech.com](mailto:pmccoy@securetech.com) was the third user to

give the malicious website sent by the compromised account, he deleted some subcategories from a website which showed that his account was also compromised

2025-02-13 at 4:20PM PST –We discovered that jball@securetech.com was the fourth user to give the malicious website sent by the compromised account, he added a wordpress plug in to the website which contains malware or malicious software which indicates that his account was compromised

2025-02-13 at 4:40PM PST –We discovered that [mbutler@securetech.com](mailto:mbutler@securetech.com) was the fifth user to give the malicious website sent by the compromised account, he created an exploit on a website which indicates his account was compromised

2025-02-14 at 8:00AM PST –We discovered that not all members of the securetech company reicved that spam and phshing email from [jrobinson@securetech.com](mailto:jrobinson@securetech.com)

2025-02-14 at 12:45PM PST –We discovered that users [mmorales@securetech.com](mailto:mmorales@securetech.com), [tprice@securetech.com](mailto:tprice@securetech.com), and [csanders@securetech.com](mailto:csanders@securetech.com), modified, delete or added stuff to other websites

2025-02-14 at 5:53PM PST –We discovered that [mmorales@securetech.com](mailto:mmorales@securetech.com) modified web content at a website after he opened the malicious link sent by [jrobinson@securetech.com](mailto:jrobinson@securetech.com) but didn’t give any information to him

2025-02-15 at 9:52AM PST –We discovered that jbarber@securetech.commodified web content at a website after he opened the malicious link sent by [jrobinson@securetech.com](mailto:jrobinson@securetech.com) but didn’t give any information to him

2025-02-15 at 1:12PM PST –We discovered that after the attack the users rblack@securetech.com, bho@securetech.com, tingram@securetech.com, drichardson@securetech.com, drichardson@securetech.com, cjohnson@securetech.com, dking@securetech.com, ssmith@securetech.com, drichardson@securetech.com, brobertson@securetech.com, mmartin@securetech.com, [jhunt@securetech.com](mailto:jhunt@securetech.com), all installed wordpress plugins to various websites which could contain malicious software

2025-02-15 at 6:12PM PST –We discovered that many users in the company received that malicious phshing link from 20 other emails beside [jrobison@securetech.com](mailto:jrobison@securetech.com) which showed that jrobinson@securetech wasn’t the only email the attacker compromised other emails outside securetech.com accessed the email, which were carmen05@gmail.com, jryan@morgan-hernandez.com, danielle36@hotmail.com, sonia98@hotmail.com, steven67@nunez-hester.net, thompsonjeremiah@stokes.com, baxterjody@hotmail.com, kimberly39@yahoo.com, gpeters@wang-fox.com, williamsmichael@gmail.com, gomezjennifer@gmail.com, david55@hotmail.com, hilljesse@jordan-ortiz.com, julie70@hotmail.com, anthonycooper@lang.com, [davistravis@larson.com](mailto:davistravis@larson.com)

2025-02-15 at 9:00PM PST –We discovered that the service redord of the malicious website was srv-61 which was part of the same dns server as the phshing message so we looked and found more websites with this server record of srv-61 which was srv-61.torres.walker.com, srv-61.sullivan-myers.andrade.com, srv-61.salinas-williams.terry.com, srv-61.fry.reyes.biz, srv-61.gill.reed-anderson.biz,

2025-02-16 at 9:16AM PST –we discovered that many of the securetech users accessed those other websites in the srv domain and users cfranklin@securetech.com, jflores@securetech.com, [eclark@securetech.com](mailto:eclark@securetech.com) gave those websites with service record 61 information which shows that their accounts could become compromised by the attacker, they gave them information and added patches to the website

2025-02-16 at 10:22AM PST –we discovered that many users who installed or added wordpress plugins and other information to different websites did it both before and after [jrobinson@securetech.com](mailto:jrobinson@securetech.com) was compromised which indicates it was part of their usual operations.

2025-02-16 at 11:23AMPST –we discovered that the email that belonged to the attacker who sent [jrobinson@securetech.com](mailto:jrobinson@securetech.com) the phishing link was carrie64@ford.com because the ip address from which the message came from was 23.74.164.69 which is the same ip address of the malicious website of srv-61.kim.johnson.biz , he only sent that email once based on the logs.

# Findings

What I found that there were many emails in the securetech company, one of the emails sent to [jrobinson@securetech.com](mailto:jrobinson@securetech.com) was unknowingly malicious and due to a lack of scanning in the accounts in the network and a lack of rules in the firewalls it let that malicious traffic of the phshing link“https://srv-61.kim.johnson.biz/login” and its ip address 23.74.164.69 pass through, smorgan@securetech.com reported a phishing message sent from jrobinson@securetech.com, we then discovered that before the user jrobinson@securetech.com with ip address 10.10.1.7 made a login into an external website way before it was reported by smorgan@securetech.com. On Febuary 7th jrobinson@securetech.com consisently and at the same time sent out emails to other users in the securetech community all of them at once, which showed that he was targeting the other employees in the company. jrobinson@securetech.com recieved emails from other outside sources prior to sending out all the emails sent to the other users in securetech like he recieved them from “[mary92@bradley-howe.info](mailto:mary92@bradley-howe.info)” ,”bbaker@hotmail.com”  , “[tommykirby@roberts.info](mailto:tommykirby@roberts.info)”, “[jtaylor@yahoo.com](mailto:jtaylor@yahoo.com)”, and many more outsider users all of which were either before or after he sent that huge spam and email to the other securetech employees. The potential phshing website started with http which indicated that this was insecure. In the http logs there was so many unsecure and unknown dns domains like .biz. Most of the SMTP connects from the malicious link of https://srv-61.kim.johnson.biz/login “ was coming from the ip address of 23.74.164.69. [jrobinson@securetech.com](mailto:jrobinson@securetech.com) did normal activity like the other securetech users did which showed that he was logged in as the legitimate user. He repeadelty sent out messages to the other users in the same ip of 23.74.164.69, he received emails from other outsiders like the other users did. Based on the mail logs [jrobinson@securetech.com](mailto:jrobinson@securetech.com) was the only user with securetech to send out emails and he only sent them to other securetech users no other user which incidates that he was targeting the securetech employees, which shows that it was a phishing attack which was lateral phishing which is targeting internal employees only ina company, which incidates that the user account [jrobinson@securetech.com](mailto:jrobinson@securetech.com) was compromised and sent a malicious email to another internal employee which encourage the internal employees to provide access to sensitive data. There was also a POST http method which showed [sritter@securetech.com](mailto:sritter@securetech.com) username which indicates that he gave sensitive or personal information to that website which showed that his account was in danger and could’ve been compromised. Earlier in the HTTP logs there was a also a POST http method which showed [jrobinson@securetech.com](mailto:jrobinson@securetech.com) which showed that his account was compromised by an attacker because he gave sensitive information and credentials based on the POST information and the attacker used that information to compromise and hack into his account and then use his account to send out that huge phishing email containing that malicious link of <https://srv-61.kim.johnson.biz/login>. No other user in the securetech domain other than [jrobinson@securetech.com](mailto:jrobinson@securetech.com) sent out an email to anyone in the securetech domain even to people outside the domain. Users jfoster@securetech.com,sritter@securetech,com bbarron@securetech.com, pmccoy@securetech.com, jball@securetech.com, and [mbutler@securetech.com](mailto:mbutler@securetech.com) gave their personal or any information to the website which they'll became a victim of phishing and they'll end up loosing some important and sensitive information which showed that there were like 6 other victims besides [jrobinson@securetech.com](mailto:jrobinson@securetech.com) and [sritter@securetech.com](mailto:sritter@securetech.com) who gave information to that malicous website of https://srv-61.kim.johnson.biz/login “ owned by the attacker who sent our those emails to the internal exployees containg the phishing link, every user who reicved an email that wasn’t from [jrobinson@securetech.com](mailto:jrobinson@securetech.com) was from outside the securetech domain which showed that all the emails that are malicious for sure were all from [jrobinson@securetech.com](mailto:jrobinson@securetech.com), but we don’t know if there are any malicious emails out there due to a lack of antivirus software link scanners in the company, [jrobinson@securetech.com](mailto:jrobinson@securetech.com) reicved an email from a outside domain after his account was compromised and sent out that long phishing email to the other securetech users which showed that the internal user whose account was compromised was actually able still able log in to his account and do his usual activities,  the actual user was logged in before his account was compromised and did his usual activities and after his account was compromised and did his usual activities, which then also showed that the attacker didn’t lock him out or change his credentials.The compromised [jrobinson@securetech.com](mailto:jrobinson@securetech.com) sent the spam at IP address  23.74.164.69, but was at wide variety of other ip addresses when he was logged in as the legitimate user when receiving his emails at different ip addresses like 158.221.111.254,68.53.24.26,99.118.240.33, while he may have not lost his credentialds or access to his account, the attacker still ruined his reputation and was trying to cover himself up by putting the blame on the account, the attacker implemented lateral phishing by logging in as [jrobinson@securetech.com](mailto:jrobinson@securetech.com) without changing any credentials and sending unusual spam emails to people close to them in the network like employees in the company. The user [jrobinson@securetech.com](mailto:jrobinson@securetech.com) opened the malicious website of <https://srv-61.kim.johnson.biz/login> way before everyone else did as the legitimate user and based on the api end point of “/login” he was forced to give a username and password which he did and the attacker who owns that website must have found his username and password and used that information to log in as securetech or if the account was different, then the user must have used the same password that he uses for his securetech account and the attacker tried that password to log into the securetech account with that password and it work which showed the dangers of using the same password again and again. While reading through the mail logs I noticed that all the emails beside jrobinson@securetech who sent a message to anther person in securetech was not a part of the secure tech domain, no other securetech email beside [jrobinsons@securetech.com](mailto:jrobinsons@securetech.com) sent an email to another securetech email which shows that is malicious and unsual activity and it was a sign of someone trying to get information from the other securetech users. When [jrobinson@securetech.com](mailto:jrobinson@securetech.com) was logged in as the legitimate user there was a POST method in the http logs at the website “srv-61.kim.johnson.biz”, there was a lack of scanning of of the urls when the compromised user accessed the website which showed that the companies vulnerability was that it opens all websites without checking if they are safe or not even if they find a vulnerable website they are providing services to, they must check the website first to see if it is safe before giving them security services. Based on POST PATCH,PUT, TRACE methods many users in the companies accessed outside websites and added plug ins or other things to the external websites both before and after the [jrobinson@securetech.com](mailto:jrobinson@securetech.com) compromise, which showed it was part of usual activites and them providing security services to websites the PUT method incidates that the securetech users replaced something at that website with something more or less secure, PATCH method incidates that the securetech users added something at that website with something more or less secure, POST method incidates that he gave information to that websit, TRACE method indicates that there are diagnostic services happening on the website and testing for some security or any vulnerabilities. The first victim who was [jfoster@securetech.com](mailto:jfoster@securetech.com) accessed another website laptop-68.miller-stanley.org, but there was no POST information which showed he didn’t harm that website, but he accessed another website of “db-89.mccall.com/posts/categories” in which there was a trace method which showed he was performing a diagnostic test on the website. After [jfoster@securetech.com](mailto:jfoster@securetech.com) opened the malicious link he then accessed more websits like laptop-68.miller-stanley.org, but gave no information or didn’t modify the website which showed that he was safe, he then accessed “db-89.mccall.com/posts/categories”, but did some testing and diagnostics on that website. After [bbarron@securetech.com”,opened](mailto:bbarron@securetech.com) the malicious link he then accessed more websites like "web-81.juarez-raymond.woodward.com/main/blog/app" were he deleted something that was based on the http DELETE method, he then accessed another website “srv-02.mcdonald.chaney-forbes.info/tags/categories”,which we replaced something possible something that was insecure with something secure based on the PUT method, he received more emails but didn’t open it. After [pmccoy@securetech.com](mailto:pmccoy@securetech.com) opened the malicious phishing link, he then opened another website which was “lt-22.graham-bates.gill.org/category/categories”, he deleted something from that website based on the DELETE http method, he then accessed another website “web-12.garcia.small.info/blog/category/categories”, in which he replaced something on the website based on the HTTP PUT method. After [jball@securetech.com](mailto:jball@securetech.com), opened up the malicious phishing link, he then accessed the website “laptop-93.mcgee-miller.com/tag/tag/category”, and there was a PUT method which shows that he replaced something on tgat website, but there was a sign his account was compromised but its not guaranteed which was when he accessed the website db-63.cook.com/tags/blog he inserted a wordpress plugin based on the endpoint /wp-content, there was a patch method which indicated that the user added something malicious to that website because many word press plugins are known to have malware in them, which could show that his account was compromised. After [mbutler@securetech.com](mailto:mbutler@securetech.com) opened the malicious phishing link he opened the website “srv-78.owens-randolph.maldonado.com”, he ran a diagnostics on this website based on the Trace method. Not all users in the secure tech company reicvieved that spam/phishing email from [jrobinson@securetech.com](mailto:jrobinson@securetech.com), other users like [latkins@securetech.com](mailto:latkins@securetech.com) didn’t receive them which showed some users in the company are safe. Anything harmful would occur at HTTP methods like POST,PUT,PATCH, and TRACE, POST sends sensitive information, PUT, Replaces information, PATCH adds information, TRACE indicates that information is being sent back and forth or potential exploits which indicate that the website could be unsafe. [jthomas@securetech.com](mailto:jthomas@securetech.com) deleted a wordpress plug in which means he was trying to delete something malicious. [mmorales@securetech.com](mailto:mmorales@securetech.com) opened a website srv-40.trujillo.garcia.com he received the scam phishing email from the compromised account but didn’t open the link since there was no GET method which shows his account was fine and wasn’t compromised. [tprice@securetech.com](mailto:tprice@securetech.com) replaced a wordpress search content with something new based on the PUT method, he didn’t receive an email from [jrobinson@securetech.com](mailto:jrobinson@securetech.com). jrobinson@securetech while compromised by the attacker couldbe done another malicious thing but not guaranteed, which was delete all categories from srv-82.adkins-hinton.romero.biz. [mmorales@securetech.com](mailto:mmorales@securetech.com) replaced something at at "laptop-86.brown.org",he opened the malicious phishing link sent by [jrobinson@securetech.com](mailto:jrobinson@securetech.com) but didn’t give that website information. I discovered that many websites the user accessed used old and outdate versions of web browsers like old versions of chrome and many of the seucretech users who were review the websites from the emails were finding that when inspecting the security of the website. [jbarber@securetech.com](mailto:jbarber@securetech.com) added a list to the website desktop-39.rios.gray.com based on the PATCH HTTP method. Users pclarke@securetech.com, jcarter@securetech.com, rblack@securetech.com. bho@securetech.com, tingram@securetech.com, drichardson@securetech.com, cjohnson@securetech.com, dking@securetech.com, ssmith@securetech.com, brobertson@securetech.com, and [jhunt@securetech.com](mailto:jhunt@securetech.com), based on the PATCH method inserting a wordpress plugin on various websites based on API endpoint wp-content, which indicates they were doing something malicious, he applied a partial updated the resource by adding a word press plugin to the website in which those potential plugins and changes to the website could contain malware which can infect their website with viruses and lead to problems, they were trying to add a plug in to a wordpress site which could be potentially malicious but its not guaranteed. Users bhowell@securetech.com and rsingleton@securetech.com , opened the malicious website at srv-61.kim.johnson.biz at the IP address 23.74.164.69, based on the HTTP GET method but they didn’t give any information to that website because there was no http post method but we should change their credentials and remove anything from their account just in case. They received that phishing scam email from jrobinson@securetech.com but opened it before most of the other users did. Many other emails were comprmised by the attacker beside [jrobinson@securetech.com](mailto:jrobinson@securetech.com), but they were all not a part of the securetech domain, the emails were carmen05@gmail.com , jryan@morgan-hernandez.com , danielle36@hotmail.com, sonia98@hotmail.com , steven67@nunez-hester.net , thompsonjeremiah@stokes.com, baxterjody@hotmail.com , kimberly39@yahoo.com , gpeters@wang-fox.com , williamsmichael@gmail.com , gomezjennifer@gmail.com, david55@hotmail.com, hilljesse@jordan-ortiz.com, julie70@hotmail.com, anthonycooper@lang.com, [davistravis@larson.com](mailto:davistravis@larson.com), all of which were external emails outside the securetech domain, and they all opened the malicious phishing link of srv-61.kim.johnson.biz at the IP address 23.74.164.69, they all sent the phishing link to the other secure tech users, the minute [jrobinson@securetech.com](mailto:jrobinson@securetech.com) was compromised the attacker found the other internal users in the company and sent all the internal users to these addresses he compromised and use these email addresses along with [jrobinson@securetech.com](mailto:jrobinson@securetech.com) to send the emails but he only accessed each of them once while most of the time he accessed [jrobinson@securetech.com](mailto:jrobinson@securetech.com) to send those spam emails to all the users in securetech. Users pgriffin@securetech.com, swaters@securetech.com, jmeyers@securetech.com, gwilliams@securetech.com, aharrell@securetech.com, bgonzalez@securetech.com, dkathleen@securetech.com, mgeorge@securetech.com, lwells@securetech.com, wsmith@securetech.com, rhorne@securetech.com, aturner@securetech.com, swatson@securetech.com, storres@securetech.com, ksanders@securetech.com, [tcooper@securetech.com](mailto:tcooper@securetech.com) all of which received an email containing the phishing link of srv-61.kim.johnson.biz at the IP address 23.74.164.69, from the external non securetech users, [jrobinson@securetech.com](mailto:jrobinson@securetech.com) was not the only affected email 20 other emails outside securetech.com were infected. [jrobinson@securetech.com](mailto:jrobinson@securetech.com) accessed the website before everyone else did and when logged in [jrobinson@securetech.com](mailto:jrobinson@securetech.com) he found a list of people in the company wrote their emails and printed it on a list and sent it to all the other compromised email addresses. The service record the malicious phishing link was apart of was srv-61, so I determined that we need to check other websites in that service record and block that service record the service record was numbered at 61, we found that there were other websites that also had that service record srv-61.torres.walker.com, srv-61.sullivan-myers.andrade.com, srv-61.salinas-williams.terry.com, srv-61.fry.reyes.biz, srv-61.gill.reed-anderson.biz all of which share the same record as the malicious phishing link which indicates they all also could be phishing links that are owned by the attacker. All of the websites are apart of the same server and domain service or DNS server. [cli@securetech.com](mailto:cli@securetech.com) accessed the website of srv-61.torres.walker.com, he just connected to the website, but we should clean out all the data and changenhis credentials just in case. [cfranklin@securetech.com](mailto:cfranklin@securetech.com) accessed the other website of srv-61.sullivan-myers.andrade.com he added something to that website based on the PATCH method which could potentially cause his account to be compromsised. jflores@securetech.com accessed the website srv-61.salinas-williams.terry.com, he then performed a loop back test along its path and was able to see all information which indicates he was testing something on the website to see if it works, but could be in danger since he did it at a malicious domain. [eclark@securetech.com](mailto:eclark@securetech.com) accessed the website srv-61.fry.reyes.biz, based on the TRACE method he performed a loop back test along it path and his account could be in danger because he did it at a malicous website, [dpotter@securetech.com](mailto:dpotter@securetech.com) accessed the website of srv-61.gill.reed-anderson.biz, which is also part of the domain, many users in the securetech company opened websites and either added, installed or deleted variety of wordpress plug ins both before and after [jrobinson@securetech.com](mailto:jrobinson@securetech.com) account was compromised which shows it may not be malicious and is part of the security services they are providing to the websites they service, [cfranklin@securetech.com](mailto:cfranklin@securetech.com) opened up srv-61.sullivan-myers.andrade.com but never received an email from jrobinson@securetech.com . [jflores@securetech.com](mailto:jflores@securetech.com) opened up srv-61.fry.reyes.biz but he never received that phishing email from jrobinson@securetech.com nor didnt send any emails to other internal users, dpotter@securetech.com opened up srv-61.gill.reed-anderson.biz but he did however receive that phishing email from jrobinson@securetech.com but he didnt open the phishing email due to a lack of a GET message. [jrobinson@securetech.com](mailto:jrobinson@securetech.com) was compromised because he used the same password for another account when he logged in to that malicious phishing website which he didn’t know was malicious and because of that the attacker used his credentials to log into the securetech company, then made a phishing attack. The email that sent [jrobinson@securetech.com](mailto:jrobinson@securetech.com) came from [carrie64@ford.com](mailto:carrie64@ford.com), because the ip address from which the message came from was 23.74.164.69 which is the same ip address of the malicious website of srv-61.kim.johnson.biz , the attackers email was [carrie64@ford.com](mailto:carrie64@ford.com), A lot of the POST, HEAD, GET methods were not encrypted and in plaintext. There was a lack of rate limiting on the securetech company due to [jrobinson@securetech.com](mailto:jrobinson@securetech.com) sending multiple messages at a time. There was also a lack of email rate limiting on the network and the software of the device which caused the user to send emails to as much users as possible.

# Actions Taken

2025-02-13 at 8:00AM PST – The company locked down all the services and servers in the company

2025-02-13 to 2025-02-16– The company had its SOC and its entire security team review the mail logs, ip addresses, and http logs in the website to determine what happened and the investigation began

2025-02-17 at 9:00AM PST – The IT specialists started to change all the credentials and passwords of the all the users in the application, even the users whos accounts were not compromised just to keep them safe

2025-02-17 at 11:00AM PST – The Cyber Security Specialists and Firewall Administrator started to create new firewalls that would block traffic from the malicious website of srv-61.kim.johnson.biz" at ip address 23.74.164.69 along any other websites and IP addresses from the other malicious websites such as 74.247.19.181, 181.236.222.92, 212.162.94.148, 118.199.27.243, 15.178.165.17 and that we should block any website with srv-61 in its domain along with any other email that’s starts with carrie64, because we know the attacker and we need to prevent him from sending that message again, we should also block the other email addresses the other compromised emails were carmen05@gmail.com , jryan@morgan-hernandez.com , danielle36@hotmail.com, sonia98@hotmail.com , steven67@nunez-hester.net , thompsonjeremiah@stokes.com, baxterjody@hotmail.com , kimberly39@yahoo.com , gpeters@wang-fox.com , williamsmichael@gmail.com , gomezjennifer@gmail.com, david55@hotmail.com, [hilljesse@jordan-ortiz.com](mailto:hilljesse@jordan-ortiz.com),

2025-02-17 at 12:00PM to 8:00PM PST – The developers then started to implement stronger security algorithms like in the company website and software, it added more encryption whenever they request a method like GET,POST, or any other HTTP methods, the developers added encryption in the IP security and whenever they plan on sending messages to a place in order to prevent man in the middle attacks. They also implemented end to end encryption

2025-02-18 at 8:00AM to 12:00PM- The developers implemented rate limiting algorithms on the users of the website to prevent users from sending multiple messages in a quick time frame, we should decrease the maxium number of messages a user can send to the server at a time in the company in order to prevent more users from receiving that phishing email. They also added some code that prevents a user from logging into a website more than 3 times.

2025-02-18 at 12:00PM to 5:00PM-The Cyber Security and IT specialists implemented antivirus software in the company of securetech to determine if they ever come across a malicious website like srv-61.kim.johnson.biz . The developers also implemented rate limting alogorithms to prevent users

2025-02-18 at 5:00PM to 9:00PM-The developers will hash and salt all the passwords in the databases of all the users just in case it prevents attackers from getting more passwords, it also provides integrity and digital signature,

2025-02-18 at 9:00PM to 11:59PM-The developers and IT specialists decided to implemented multi factor autnetication on all of the user accounts in the company to prevent any unauthorized accounts like compromises others account because due to a lack of multifactor authentication, the attacker was able to compromise the [jrobinson@securetech.com](mailto:jrobinson@securetech.com) account.

2025-02-19 at 12:00AM to 12:00PM- The IT specialists, Cyber Security Specialist(cyber forensic analysts, penetration testers, SOCs, Ethical Hackers) decided to install some data backups and hired some cyber forensic analysts to help recover the lost and stolen data based on the HTTP logs. The IT specialists had to manually recover the data that was lost and stolen by the hijacked accounts which were [jrobinson@securetech.com](mailto:jrobinson@securetech.com), sritter@securetech.com, jfoster@securetech.com, bbarron@securetech.com, pmccoy@securetech.com, jball@securetech.com, and [mbutler@securetech.com](mailto:mbutler@securetech.com), all of which based on the POST methods gave information to that malicious website and may have their accounts compromised and data stolen or lost, none of the 5 users who gave that website information didn’t send out emails to other users if there accounts were compromised or after they gave the attacker information, because of this the IT specialists had to manually recover the data that was lost and stolen by looking at past logs, they had to restore the modified data to its original state, they had to look at the http and mail logs to determine what was the original state the users message, they had to manually rewrite all of the users information and other documents on their accounts, the users who gave information didn’t have their accounts send information to other users. They rewrote it based on the old logs, they found some data that were modified in those 5 accounts so they had to restore it to its original states

2025-02-19 at 12:00PM to 6:00PM – The developers worked on algorithms on preventing and limiting brute force attacks in the software of the securetech company in order to prevent attackers from gaining access to the software and the user accounts in the company, they also must develop email filtering algorithms to check to see if they are malicious or not

2025-02-19 at 6:00PM to 10:00PM – The Network Operators had to configure all the routers and switches in the company by adding more security features and authentications to prevent any unauthorized access to the netwroks

2025-02-19 at 10:00PM to 12:00AM –The IT specialists will then add biometric authentication on the users to add an extra layer of security

2025-02-20 at 12:00AM to 12:00PM – The cyber security specialists, it specialists and developers will remove any external plugins like malicious word press plugins or any other things that were added during the account compromise to the other users, it will review all the accounts but first it will review the six compromised accounts if there were any other plugins or any other things or software that were installed in its systems and accounts and if there were then the the cyber security specialists will delete those external plug ins and software.

2025-02-20 at 12:00PM- The administers in the company made a mandatory rule to make sure all users change their password annually

2025-02-20 at 12:00PM to 1:00PM- The IT specialist implemented an Intrusion Detection System from any malicious IP address based on Geographical scanning

2025-02-20 at 1:00PM to 3:00PM-The developers implemented a CAPTCHA turing on its software in order to prevent any bots from logging into the securetech company servers and systems

2025-02-20 at 3:00PM to 5:00PM-The IT specialists restricted access of each user account to their specific ip address and implemented remote shell log in with authentication, they will only allow their employees to do any security related and work stuff on a single laptop designated for that user, they won’t allow their employees to do work on a sperate like the personal laptops because they don’t want their personal devices or any external devices to be broken or at risk of not working. The IT specialists also blocked the IP address of that malicious website and the emails of carrie64

2025-02-20 at 5:00PM to 9:00PM-The IT specialists will implement forensic scanners on all the servers to make sure we scan for any malware or malicious networks, they will also add email scanners

2025-02-20 at 9:00PM to 12:00PM- We must also implement stronger emal scanners to determine if it is a phishing email, if the email is safe, or if the email is malicious

2025-02-21 to 2025-02-26- The company IT security team which consisents of ethical hackers, penetration testers, SOC, etc conducted an security audit to find any other vulnerabilities in the companies software and networks and determine how we should strengthen the defenses against the cyber attackers.

2025-02-27- The company mandated all employees and users of securetech to take a mandatory cyber security course

2025-02-28- The SOC finished this Incident Report and sent it to the company along with the FBI and Homeland Security

2025-02-29- Everything in secure tech was fixed, everything was resolved and fixed. Everything was updated and all the servers and users were back up live and doing their normal activities.

# Financial Impact

|  |  |
| --- | --- |
| Item | Cost |
| The document itself | $10 |
| Developer labor1 | $22,400 |
| Cyber Security Specialist labor2 | $15,000 |
| Network Specialist labor3 | $4,400 |
| IT Specialist labor4 | $34,400 |
| Costs of Installing firewalls5 | $500 |
| Business down time cost7 | $384,000 |
| Multi Factor Authentication8 | $1,000 |
| Installing Anti Virus Software6 | $10,950 |
| Email scanners9 | $1,000 |
|  |  |
| Total | $466,710 |

1. The developers must change the logic, infrastructure, add antivirus software, they must implement stronger security algorithms in the code, the developers should add hashing and salting to the passwords, there were 5 developers who worked overtime, the average pay for a developer working to fix the damages from a cyber attack is $140 /hr, the developers worked for 32 hours, so 5 \* 32 \* 140 = $22,400
2. The cyber security sepecialits must analyze the problems, do some penetration techniques, secure the devices and networks on the devices there were 5 cyber security specialsits who worked overtime, they worked for a total of 25 hours and their average pay is $120/hr if they are fixing damages from a cyber attack so 5 \* 25 \* 120 = $15,000
3. The networking speciliasts must fix the servers, implement firewall rules, configure the routers and switches, there were 8 netwroking specialists who worked overtime, each network specialist worked 5 hours and there average pay to fix damage from a cyber attacker is $110/hr, so 8 \* 5 \*110 = $4,400
4. The IT specialists must add some data backups, install some firewalls, install multi factor authentication, remove any malicious software they find like any malicious plug in or not, there are like 8 IT specialists, they worked 43 hours they are paid $100 /hr to fix damages from a cyber attack, so 8 \* 43 \* 100 = $34,400
5. It costed like $100 dollars to install for each new firewalls , which are 5 firewalls so 5 \*100 = $500
6. The average cost of installing antivirus software is $30/year so 30 \* 365 = $10,950
7. The average business downtime cost is $1,000 dollars per hour and since business was down for 16 days it would be 24 \* 16 \* 1,000 = $384,000
8. The average cost for installing multi factor authentication is $1,000
9. Email scanners cost about $1,000 to implement on the servers and networks of the company

# Lessons Learned

## Successes

* Whenever there is a POST request we know that someone gives out information to that website, because of that we found the root cause of the phishing attack, which was a user giving out information like his credentials which caused his account to be compromised
* We found out the attackkers email based on the malicious websites IP address and we decided to block that account from ever sending messages on the servers again and that IP address on the server again
* The compromised accounts credentials weren’t changed by the attacker but we changed his credentials just in case if the attacker ever tried to log in again
* no other user send out a so many emails like [jrobinson@securetech.com](mailto:jrobinson@securetech.com) did
* We learned not all POST, TRACE,PUT or PATCH methods are bad many of the securetech users do it to add security things to the website they provide service to, but its any easy way to find out what the problem was
* All the people who gave that malicious website information didn’t later send out a huge long list of messages, which showed that their accounts weren t compromised and that they were safe
* All the users in the company went through a mandatory security training and change of credentials

## Opportunities for Improvement

|  |  |  |
| --- | --- | --- |
| Issue | Recommendation | Action Item Owner |
| Lack of Firewall rules | Add more firewall rules that restrict ip addresses from malicious websites, unsecure websites, | Cyber Security Specliasts, IT Specialists, and Networking Specialists |
| Lack of Antivirus software | Install Antivirus software that detects any malicious or unsecure websites | Cyber Security Specliasts, IT Specialists, and Networking Specialists |
| Lack of Rate Limiting | Develop algorithms that have rate limiting in which it limits the user from sending to many messages at a time and because of the lack of rate limiting the user spammed and sent out the emails continuosly | Developers |
| Lack of Multi Factor Authentication | Due to a lack of MFA the attacker was able to log into the [jrobinson@securetech.com](mailto:jrobinson@securetech.com) account and because of this his account was compromised | IT Speciliasts |
| Users Should not use the same passwords everywhere | Because [jrobinson@securetech.com](mailto:jrobinson@securetech.com) logged into that website potentially with the same password and credentials the attacker brute forced it | Everyone |
| We need to enable email filtering and scanning | Due to a lack of email filtering and scanning, many potentially malicious emails are being sent to the users in secure tech | IT Specialists |