servicenow

Now on Now: How the Now Platform transformed our security incident phishing response

Automation saves time and cost, and boosts analyst productivity by 40%

Table of Contents

Introduction

Phishing is a growing cybersecurity challenge in which scammers send seemingly legitimate emails intended to lure recipients into clicking a link and providing personal data such as login credentials or credit card information.

In our personal lives, the risk is primarily to the individual. In the corporate world, however, a phishing attack can compromise the entire enterprise. That's why ServiceNow runs a rigorous program to help detect, analyze, and eliminate phishing threats. Employee awareness plays a key role in this effort, so we also conduct regular phishing awareness training that includes sending mock phishing emails, tracking responses, and providing feedback.

With phishing, as with all security-related activities, time is of the essence. To stay ahead of this growing threat, we automated our phishing response using our Security Operations product running on the Now Platform®.

Our Journey to Success

In the past, when a phishing notification came in, a Security analyst would process it manually, investigate the potential threat, send an update to the employee, and close the ticket. This approach had multiple challenges:

- **Efficiency** – The response process did not scale—it was manual, inefficient, and time-consuming.
- **User communication** – Follow-up with users who alerted Security about a potential phishing email was inconsistent and delayed.
- **Analyst productivity** – The process took Security analysts' time away from other serious security threats.
- **False positives** – Most reports turned out to be spam or legitimate emails, rather than actual phishing attacks, so time was lost.
- **Workload spikes** – Analyst workloads were on the rise due to the company's rapid growth and increased dramatically during quarterly internal phishing campaigns, particularly in October, which is security awareness month (see figure 1).

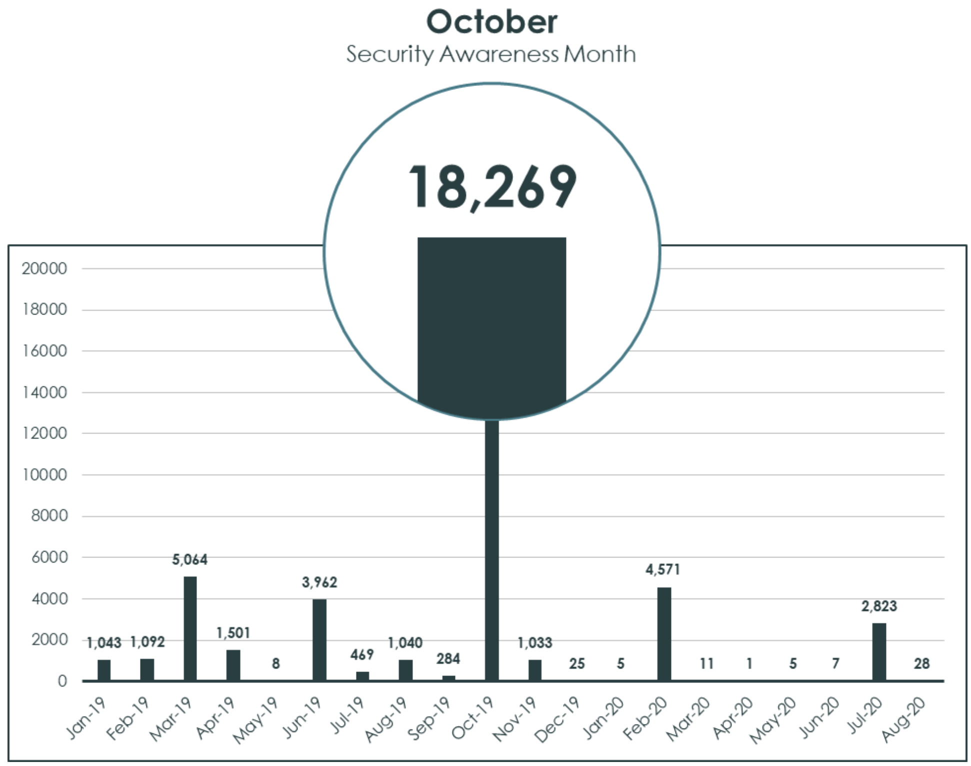


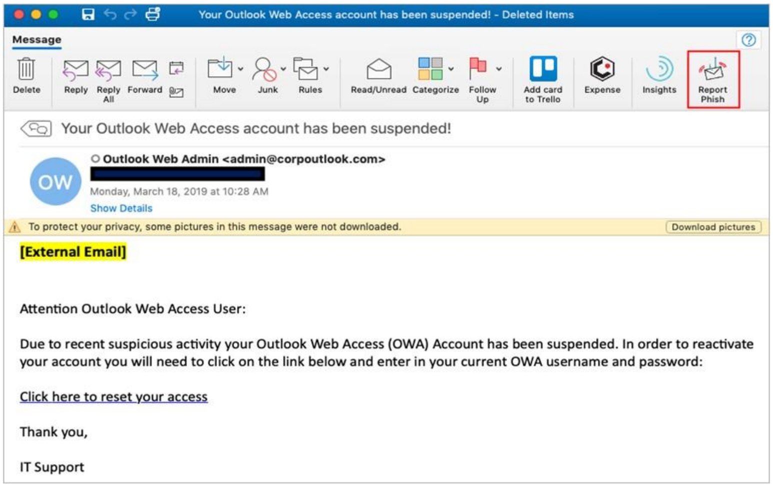
Figure 1 Internal Campaign Responses

The Security team knew there had to be a better way and turned to our own Security Operations product and the Now Platform.

Phase 1 – Workflow Automation

In 2018, we automated our phishing response process:

When a user spots a possible phishing email, they click the *Report Phish* button in Outlook. The system then creates a security incident and initiates a workflow.



Your Outlook Web Access account has been suspended!

Outlook Web Admin <admin@corpoutlook.com>
[redacted]
Monday, March 18, 2019 at 10:28 AM

To protect your privacy, some pictures in this message were not downloaded.

[External Email]

Attention Outlook Web Access User:

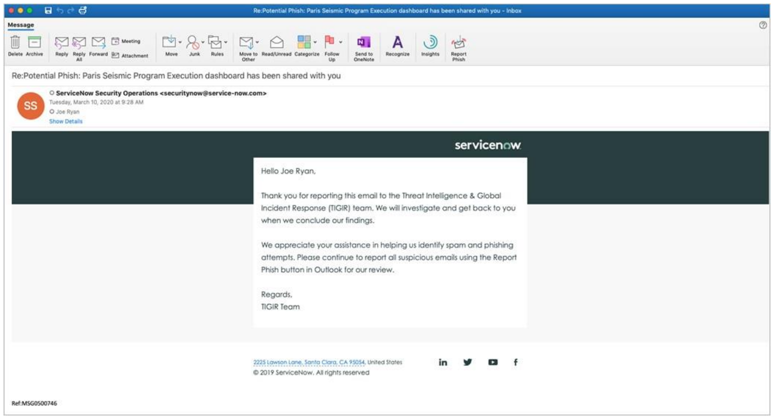
Due to recent suspicious activity your Outlook Web Access (OWA) Account has been suspended. In order to reactivate your account you will need to click on the link below and enter in your current OWA username and password:

Click here to reset your access

Thank you,

IT Support

The system sends a response to the user thanking them for their submission and telling them that the email is being investigated. The system then creates a task and sends it to a Security analyst for investigation.



Re:Potential Phish: Paris Seismic Program Execution dashboard has been shared with you

ServiceNow Security Operations <securitynow@service-now.com>
Tuesday, March 10, 2020 at 9:28 AM
Joe Ryan

Hello Joe Ryan,

Thank you for reporting this email to the Threat Intelligence & Global Incident Response (TIGIR) team. We will investigate and get back to you when we conclude our findings.

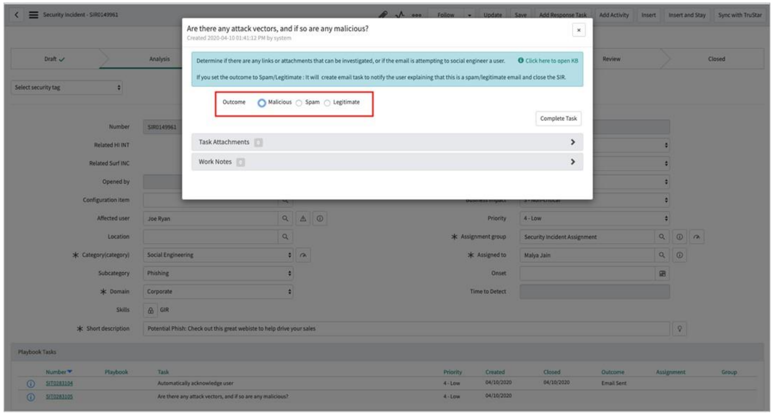
We appreciate your assistance in helping us identify spam and phishing attempts. Please continue to report all suspicious emails using the Report Phish button in Outlook for our review.

Regards,
TIGIR Team

2225 Lawson Lane, Santa Clara, CA 95054, United States
© 2019 ServiceNow. All rights reserved

Ref:MSG0500746

The analyst opens the task, evaluates the email, and selects one of three outcomes: malicious, spam, or legitimate.



Are there any attack vectors, and if so are any malicious?
Created 2020-04-10 01:41:12 PM by system

Determine if there are any links or attachments that can be investigated, or if the email is attempting to social engineer a user. Click here to open KB

If you set the outcome to Spam/Legitimate : It will create email task to notify the user explaining that this is a spam/legitimate email and close the SIR.

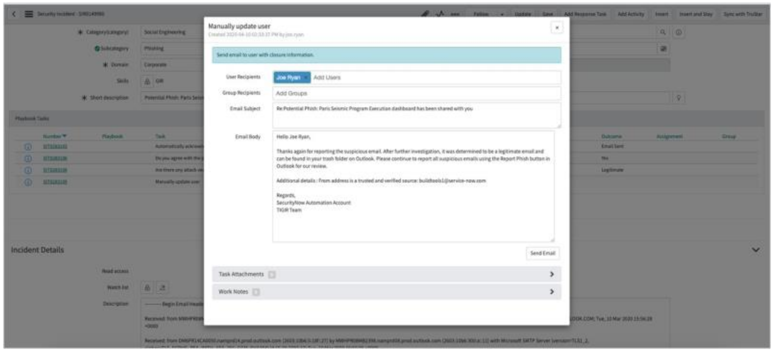
Outcome ○ Malicious ○ Spam ○ Legitimate

Number	SIR0149961
Related HI INT	
Related Surf INC	
Opened by	
Configuration item	
Affected user	Joe Ryan
Location	
Category(category)	Social Engineering
Subcategory	Phishing
Domain	Corporate
Skills	GIR
Short description	Potential Phish: Check out this great webiste to help drive your sales
Priority	4 - Low
Assignment group	Security Incident Assignment
Assigned to	Malya Jain
Onset	
Time to Detect	

Playbook Tasks

Number	Playbook	Task	Priority	Created	Closed	Outcome	Assignment	Group
SIT0283104		Automatically acknowledge user	4 - Low	04/10/2020	04/10/2020	Email Sent		
SIT0283105		Are there any attack vectors, and if so are any malicious?	4 - Low	04/10/2020				

Depending on the analyst's choice, the system prepopulates a message to the user telling them the results of the investigation. The analyst edits the message if desired and clicks "send."



Manually update user

Send email to user with closure information.

User Recipients: Joe Ryan
Group Recipients: Add Groups
Email Subject: Re:Potential Phish: Paris Seismic Program Execution dashboard has been shared with you
Email Body:

Hello Joe Ryan,

Thanks agin for reporting the suspicious email. After further investigation, it was determined to be a legitimate email and can be found in your trash folder on Outlook. Please continue to report all suspicious emails using the Report Phish button in Outlook for our review.

Additional details : From address is a trusted and verified source: buildtools1@service-now.com

Regards,
SecurityNow Automation Account
TIGIR Team

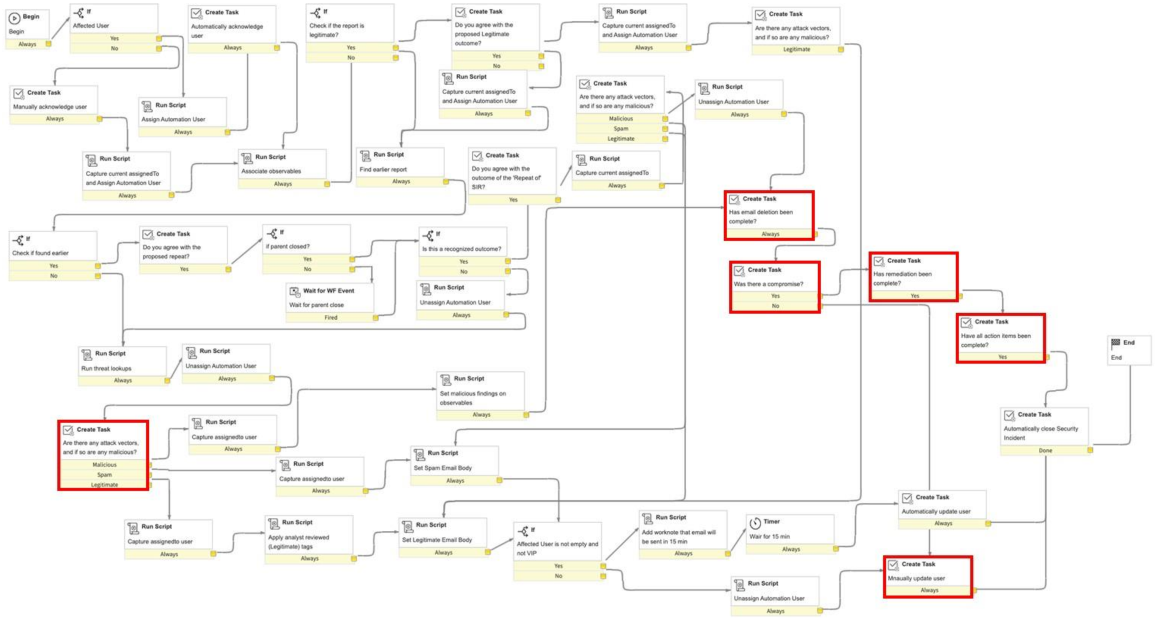
If the submitted email is spam or legitimate, the system logs the status and closes the ticket. If the email is malicious, the system updates the task with relevant Knowledge Base articles and prompts the analyst to take action.

Phase 2 – Workflow Enhancement

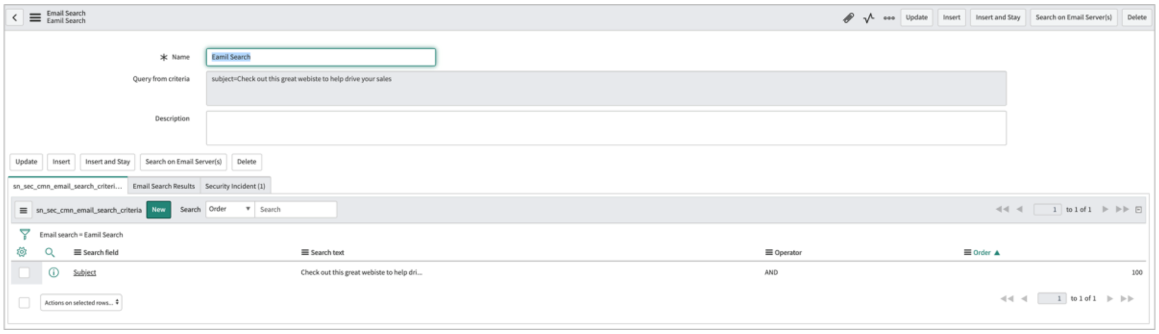
After using the automated workflow for several months, the Security team identified several opportunities for further automation and improvement:

- **Internal phishing campaigns** – Because we know the subject and content of the testing emails and when Security will send them, we can make this a zero-touch workflow.
- **Multiple identical submissions** – Sometimes multiple users submit the identical email to the Security team. Once a Security analyst handles the first submission, the system can identify duplicate submissions and, using the analyst's actions with the first submission, manage those responses automatically.
- **Known legitimate emails** – Users often report legitimate emails, particularly during internal phishing campaigns when users are on the lookout for phishing attacks. By creating a *whitelist* of known legitimate emails, the system can compare submissions against that list, identify safe ones, and handle user responses.

Now that these improvements are in place, a huge portion of our phishing response workflow has been automated. Only a few steps require analyst support (see workflow below with manual steps in red).



Because the Now Platform provides seamless integration of our security applications with third-party tools, analysts have a single screen for managing phishing emails. Built-in communication lets analysts message users without exiting the Now Platform.



∗ Name: Eamil Search

Query from criteria: subject=Check out this great webiste to help drive your sales

Description:

Email search = Eamil Search

Search field	Search text	Operator	Order ▲
Subject	Check out this great webiste to help dri...	AND	100

Benefits

Digitizing workflows has provided qualitative and quantitative benefits to ServiceNow.

- **Analyst productivity** – The Now Platform puts communications and security tools at analysts' fingertips, which has increased productivity by 40%. Automated workflows also give analysts more time to focus on other critical security work.
- **Time and cost savings** – Automating our phishing response saves nearly 2,100 hours or approximately $150,000 per year.
- **Speed, accuracy, and efficiency** – We've seen a dramatic improvement in the speed, accuracy, and efficiency of our phishing response.
- **User communication** – Users receive prompt notifications that give them the assurance that their phishing submissions have been received and are being addressed.

To learn more

- Explore the ServiceNow Security Operations web page.
- Browse the ServiceNow Community forum for Security Operations to get tutorials and insights on phishing and other security-related topics.

About ServiceNow

ServiceNow is making the world of work, work better for people. Our cloud-based platform and solutions deliver digital workflows that create great experiences and unlock productivity for employees and the enterprise. For more information, visit www.servicenow.com.

Now on Now is about how we use our own ServiceNow solutions to work faster, smarter, and better. With Now on Now, we're achieving true end-to-end digital transformation. To learn more, go to www.servicenow.com/nowonnow.