

Microsoft Attack Simulation Training powered by **sepago** Customer Case Study

SEPAGO IN A NUTSHELL



SYSTEM INTEGRATOR,
ISV AND CLOUD MANAGED
SERVICE PROVIDER



SINCE 2002

SUCCESSFUL ON THE MARKET
AT THREE LOCATIONS:
COLOGNE HAMBURG MUNICH



SPECIALISED IN

MICROSOFT CLOUD TECHNOLOGIES, MODERN WORKPLACE,
MOBILITY, APP VIRTUALISIERUNG & VDI, CITRIX WORKSPACE
APP, VIRTUAL MANAGED SERVICES, IT CHANGE MANAGEMENT
& IT-SECURITY



**HUNDREDS OF
SATISFIED
CUSTOMERS**



85 ENTHUSIASTIC EMPLOYEES

EXCELLENT ORGANIZATIONAL CULTURE
COMMUNITY AWARDS



**MILLIONS OF GOOD
IDEAS**

MICROSOFT ATTACK SIMULATION TRAINING POWERED BY



*sepago accompanies the pre-operation phase **continuously** and in a **procedurally structured** manner based on **blueprints and templates** to set-up the Microsoft Attack Simulation Training for **efficient and effective** cyber security phishing campaigns.*

THE COMPANY

- small, Germany-based automotive manufacturing company (MDAX-based)
- 25.000 employees generated about 2,5 billion € in 2020

Current Challenge:

Customer has just introduced new Microsoft 365 Defender suite. But their employees are not yet mature enough to recognize malicious emails and files, attacks are prevented by the Defender solutions.

The CISO wants to implement an Attack Simulation Training, but does not know, how and where to start.



WHAT WE DELIVERED

Using the Microsoft Attack Simulation Training included in Microsoft Defender for Office, we have guided the customer through the trainings:

- I. **Structured campaigns with a security phishing awareness process.**
- II. **The right training materials in the right context for the right people.**
- III. **The interpretation of the campaign results and appropriate next steps.**



AGENDA OF THE ENGAGEMENT

Kick-off-Phase

- Tool demo
- Process assessment
- End-user Reward model

Monitoring & metrics set-up

- Measurement plan/ Scorecard
- Dashboard implementation
- API connection to Microsoft PowerBI

Process & Implementation guidance

- Development & documentation operational model/ process
- Development & documentation technical Implementation plan
- Development Phishing Awareness Communication plan & material
- Roll-out Microsoft Attack Simulation & Training

Continuous support in Microsoft Attack Simulation & Training

- Initial campaign set-up
- Continuous campaign set-up
- Monitoring of results
- Recommendations of improvements & next steps

MICROSOFT ATTACK SIMULATION TRAINING

Attack simulation training

Overview Simulations **Playbooks** Automations

Playbooks are phishing emails and webpages that you use to launch simulations. You can manually create playbooks, or collect them automatically with automations.

Sort Help 52

Send a test Create a playbook Copy playbook

Applied filters

Playbook name	Type	Source	Simulations launched	Completion rate (%)	Created by	Last modified	Deactivate
2 Failed Messages	Social Engineering	Global	1	30	Microsoft	1/15/2020, 10:52:05	Deactivate
Accounts payable document review	Social Engineering	Global	0	20	Microsoft	1/12/2020, 10:04:42	Deactivate
American express password reset	Social Engineering	Global	0	45	Microsoft	1/12/2020, 10:04:48	Deactivate
American Express phone number confirmation	Social Engineering	Global	0	17	Microsoft	1/12/2020, 10:04:48	Deactivate
Applied Complete Invoice	Social Engineering	Global	0	17	Microsoft	1/12/2020, 10:04:47	Link to Help
Approval Requested/Notification	Social Engineering	Global	0	30	Microsoft	1/12/2020, 10:04:58	Link to Help
Blocked Facebook account	Social Engineering	Global	0	32	Microsoft	2/24/2020, 14:15:23	Link to Help
Capital One bank account locked	Social Engineering	Global	0	36	Microsoft	1/15/2020, 10:04:28	Deactivate
Claim a fax document	Social Engineering	Global					
Confirm account for deposit	Social Engineering	Global					
Contra Visa Stimulus	Social Engineering	Global					
COVID-19 payroll adjustment	Social Engineering	Global					
Defunct medical payment	Social Engineering	Global					
DHS Parcel tracker	Social Engineering	Global					

COVID 19 payroll adjustment

Social Engineering: Credential Harvest

Overview Simulations launched

All staff & employees of are expected to verify their email account for new payroll directory and adjustment for this month benefit payments. Please verify this...
URGENT: VERIFY YOUR CREDENTIALS
 and complete the required directive to avoid initiation of your benefits payments for this month.

Thank you,
 Payroll Administration

Playbook Description
 This payroll stubs like it comes from an admin in a corporate payroll office asking the user to update their email account for a COVID-19 related employment benefit.

From name: Christopher Lechner
 From Email: Christopher.Lechner@GLOBAL.acad

Add Training

0 training(s) selected

Recommended All trainings

25 Items Search

Training name	Source	Duration (mins)	Preview
Introduction To Infor...	Global	7	Preview
Business Email Comp...	Global	7	Preview
Email	Global	7	Preview
Identity Theft	Global	7	Preview
...	Global	7	Preview
...	Global	7	Preview
...	Global	7	Preview
...	Global	7	Preview

Identify all the four methods you can use to identify which of Global's employees to target.



Reconnaissance

Identify employees on social media networks
 Select a recipient at random
 Collect press releases
 Consult conference attendee lists
 Visit Global's website
 Send an email to all Global employees

[Submit](#)

How would you do that?

© 2020 Temasek SkillsFuture Corporation, in partnership with Microsoft



Doctor Lewis, you were just **phished**.

It's okay! You're a human. Let's learn from this.

Rather than stealing your credentials like a cyber criminal, your IT team has redirected you to this educational page instead and assigned you some training material.

Please note: Trademarks and logos used in the below email are the property of their respective owners. They are used in this email for identification purposes only and are in no way associated or affiliated with this email.

From: Microsoft Outlook <no-reply@main-es.com>

To: [Redacted]

Subject: **Spelling and grammar irregularities**
 Spelling or grammar errors, incorrect phrases and so on

Close Preview Help

Hello [Redacted]

You have some messages that has been placed on hold

This mail was sent to: doctor@sunmynetworks.net

[Review Messages Here](#)

Sincerely,
 Microsoft Customer Care

Microsoft | Support | Privacy Policy
 Copyright © 2020 Microsoft, Inc.

Microsoft Outlook WebApp 

GUIDANCE BY SEPAGO

 1_MicrosoftAttackSimulator.docx
 Implementation_ _PM (export).xls
 Implementation_Communicationplan.xlsx
 Implementation_Transformationmap.pptx
 ManagementSummary_ _MicrosoftAttackSimulator.docx
 Process_Campaignplan.xlsx
 Process_End-user survey.xlsx
 Process_Improvementlist.xlsx
 Process_Layer1_HighLevel.vsdx
 Process_Layer2_Action Items_process.xlsx
 Process_UX measurement plan.xlsx

Content	
1 Introduction	5
2 Implementation: Transformation map & Gantt-diagram	6
3 Implementation: Removal guide for Cofense button	8
3.1 Removing the Add-In for All Users inside Office 365.....	9
3.2 Removing the Add-In for All Users inside Exchange 201X.....	10
4 Implementation: Implementation guide for report-add in	11
4.1 Implementing the Report Message add-in by Microsoft.....	11
4.2 User submission policy.....	13
5 Implementation: Report Dashboard in SharePoint	18
6 Implementation: Communication plan	18
7 Implementation: Communication material	19
7.1 SharePoint text end-user.....	19
7.2 Yammer Announcement text end-user & DW early adopter.....	22
7.3 Email notification end-user.....	23
7.4 Announcement text Cyber Defence Team/Operational teams.....	24
7.5 Reminder Announcement text Operational teams & function guide.....	27
8 Process	28
9 Process: Visio high-level	29
10 Process: Action Items & step-by-step	30
10.1 Preparation yearly (Trigger: calendar year).....	30
10.1.1 Editorial calendar.....	30
10.1.2 Campaign plan (document).....	33
10.2 Campaign monthly (Trigger: calendar month).....	33
10.2.1 Choose topic based on campaign plan.....	33
10.2.2 Check targeted AD group.....	34
10.2.3 Check education landing page.....	35
10.2.4 Test run.....	36
10.2.5 Set-up campaign in Attack Simulator.....	37
10.2.6 Inform necessary stakeholder.....	40
10.2.7 Campaign runs for 7 days.....	42
10.3 Campaign review monthly (Trigger: end of campaign/month).....	43
10.3.1 Share PowerBI report on SharePoint.....	43
10.3.2 Meeting to review the last campaign if required.....	44
10.4 Extra processes: Awareness & service review (Trigger: calendar year).....	46
10.4.1 Process: Continuous reporting, review & improvement process.....	46
11 Microsoft Attack Simulator documentation	48
11.1 Attack Simulator Overview.....	48
11.2 Step-by-Step: Creating a custom payload.....	50
11.3 Step-by-Step: Creating/Scheduling a Simulation.....	54
11.4 Step-by-Step: Cancel a scheduled simulation.....	59
12 Process: Campaign plan Q3+Q4 2021	60
13 Process: Communication templates & material	61
13.1 Test information mail.....	61
13.2 Info Mail Stakeholder.....	62
13.3 Landing page educational.....	63
13.4 FAQ Phishing.....	64
13.5 Header/Body training.....	67
15 Reward for compliance model	68
16 End-user survey for sentiment analysis	70
17 Process: Monitoring	71
17.1 Measurement plan & end-user KPI structure.....	71
17.2 Process monitoring in PowerBI.....	71

OUTCOME FOR THE CUSTOMER

- Compared to before the engagement, we were able to **reduce the amount of employees clicking on malicious files and mails by 45%**
- Employees liked the **approachable and personal training experience** and the gamification aspect
- Security operations resources can be allocated to different cyber defence areas – **less noise in Microsoft Defender 365**



THANK YOU FOR YOUR ATTENTION!

Let us hear from you!

