Using Frequent Clickers to Strengthen Your Phishing Awareness Program

Mark Alexander and Heather Smee - Westfield
Mark Alexander, Security Education & Awareness

Mark has worked for Westfield for 3 years promoting information security education and awareness activities. He has conducted phishing exercises for Westfield for the last 2 years and has implemented a phishing outreach program for frequent clickers. Prior to his engagement with Westfield, Mark worked as an Instructional Technologist with Indiana University in Indianapolis.

Heather Smee, Information Security Governance, Risk, & Compliance Leader, CISSP, AINS

Heather Smee is an Information Security Professional with 17 years of experience in the Insurance Industry. In 2011 she joined the Information Security team and since 2016 she has been managing the information security governance and compliance function for the organization.

Areas of focus include security education and awareness, regulatory compliance, development and execution of the vendor security program, policy and standard stewardship, and access management governance.
It's your life. We're here to protect what's yours.
Our History

AGENCY

OHIO FARMERS INSURANCE CO.

ORGANIZED 1848
LE ROY OHIO
Our Story

- Established in 1848
- 2,600 Employees
  - Home Office = 1,600
  - P&C in 21 states
  - Surety business in all 50 states
Our Golf Course
why westfield

The insurance industry is incredibly multi-faceted. It challenges you every day to know the ins and outs of the business, understand your clients' needs and navigate the best course of action. People's livelihood is in your hands.

When you work at Westfield, you'll be inspired to learn new skills, show your strengths and grow in your career. And we give you what you need to thrive, offering competitive compensation and onsite training and development programs to help you develop the career you've always dreamed of.

Build your future...while protecting theirs.

A Relationship-Oriented Company

Our success is a direct result of great relationships – within our walls, with our agents and customers. As we move forward, we recognize those relationships are paramount to our longevity. The fact is, there are many ways to evolve a company, but at Westfield, there's only one way – together.
Back to Reality!

Time since last click on a phishing link

0d : 2h : 41m : 38s

Record

7d : 22h : 34m : 54s
Westfield Starts Phishing Exercises

2017 CLICK RATE IN REVIEW

<table>
<thead>
<tr>
<th>Scenario</th>
<th>Click Rate</th>
</tr>
</thead>
<tbody>
<tr>
<td>January</td>
<td>20.6%</td>
</tr>
<tr>
<td>February</td>
<td>11.6%</td>
</tr>
<tr>
<td>March</td>
<td>8.9%</td>
</tr>
<tr>
<td>April</td>
<td>2.6%</td>
</tr>
<tr>
<td>May</td>
<td>5.4%</td>
</tr>
<tr>
<td>June</td>
<td>6.0%</td>
</tr>
<tr>
<td>July</td>
<td>12.4%</td>
</tr>
<tr>
<td>August</td>
<td>8.2%</td>
</tr>
<tr>
<td>September</td>
<td>5.7%</td>
</tr>
<tr>
<td>October</td>
<td>28.2%</td>
</tr>
<tr>
<td>November</td>
<td>0.9%</td>
</tr>
<tr>
<td>December</td>
<td>3.32%</td>
</tr>
</tbody>
</table>
The Repeated Click Rate Went Down Quickly ....but then we looked a little bit harder.
At Westfield 53% of people tested never clicked on a phishing simulation but 7% of individuals were found susceptible in 3 or more simulations.

...and we looked a little bit harder.
And Then We Found....

click Click CLICK

CLICKETY-EFFING-CLICK
# Frequent Clickers

This table lists the names of frequent clickers and their corresponding phishing scenario dates and whether they clicked on any links.

<table>
<thead>
<tr>
<th>Name</th>
<th>Phishing Scenario Date</th>
<th>Clicked</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vendor X</td>
<td>January</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>January 2</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>February</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>February 2</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>March</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>March 2</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>April</td>
<td>X</td>
</tr>
</tbody>
</table>

... and it just kept going and going.....
We Were Faced With Choices
We Needed To Consider Our Culture

Since 1848, a lot has changed. And a lot hasn’t.

Before there were cars, electricity and television, Westfield was providing insurance protection and serving customers, achieving a level of trust and respect that remains the hallmark of how we conduct our business today.

Westfield has always been a relationship company, sharing what our employees and agents know to help customers protect the things they care about most. Our business relies on the strength of our relationships as much today as it did in 1848, when a small group of community leaders formed an insurance company to protect the property of local farmers. Our success is achieved because we believe in the ability of real people, who possess specialized knowledge, to create real value for our customers.
We Asked Ourselves...

Can 'Serial Clickers' be 'cured'?
Welcome to Phishing Forum

Lance Spitzner (SANS Institute) • 3 yrs ago • 416 • 19

Krebs - "should failing phish tests be a fireable offense?"

Meredith Howland • 7 days ago • 9 replies • 122 • 7 • Last reply 2 hrs ago

Phishing Policy

Stephanie Pratt • 4 wk ago • 25 replies • 181 • 3 • Last reply 3 days ago
The most significant learning happens at the 4th response!

Gather feedback on your training program, you may be shocked by what you hear.
Additionally, I would highly caution the approach of "disciplinary" action on users. It is a training program. If your child was having difficulty in school - would you immediately assign them more training if they were having difficulty grasping a concept? No, you would likely sit down with them and find out where the knowledge gap is.

I can't stress enough that applying any additional "training" prior to allowing the user to learn, will most times create negative feelings towards both your program (security awareness, which we here are all very sensitive about) and your department (information security).
Collaboration with HR, Procurement & Legal

• Clicking on 3 phishing exercises during a 12 month time period will prompt enrollment in the Phishing Awareness Outreach Program consisting of a brief monthly inform designed to assist in detecting malicious emails.

• Clicking on 5 phishing exercises during a 12 month time period will result in a meeting with a member of the information security team to discuss the risk associated with phishing and steps that can be taken to help improve response to these exercises.

• Clicking on 7 phishing exercises during a 12 month time period will result in an escalation to the employee’s leader with a request to discuss strategist for improvement in this area.
The Email

To: [Redacted]

Retention Policy  120 Day Retention - All Folders (4 months) Expires  10/2/2019

Dear [Redacted],

Westfield views phishing as a serious threat to its information assets.

We've noticed that you have clicked on 3 emails containing suspicious links or attachments during the last 12 months of Westfield’s phishing awareness campaign.

The last time you clicked on one of our exercises was during May of 2019 and prior to that you clicked on 2 other phishing attempts during July and November 2018. This type of behavior can infect your computer and our network with malware.

Please don’t panic. This is not intended to be punitive. We want to assist you in identifying these threats and are including you in our Phishing Awareness Outreach Program which will provide brief monthly communications to help you recognize these threats. Please make sure to read these as they will help you identify Westfield’s phishing exercises.

We also encourage you to attend one of Information Security monthly Phishing Awareness sessions that are held in both face-to-face and WebEx formats. Please consult the Information Security Awareness Calendar for available dates and times. If you prefer more personal attention please feel free to reach out to InfoSecAwareness@westfieldgrp.com to schedule a one-on-one consultation to help make improvements in this area. We will be happy to work with you.

The Phishing Escalation Process is as follows:

- Clicking on 3 phishing exercises within a year will automatically subscribe you to the Phishing Awareness Outreach Program.
- Clicking on 5 phishing exercises within a year will result in a meeting with a member of the information security team to discuss the risk associated with phishing and steps that can be taken to help improve your response to these exercises.
- Clicking on 7 phishing exercises in a year will result in an escalation to your leader with a request to discuss strategies for improvement in this area.

To learn more about phishing, visit the Information Security WeConnect phishing resources page which includes examples of phishing emails, as well as informational resources that can be used to help identify malicious emails. Please feel free to respond back with any questions that you may have.
The Outreach Letter

Mon 11/12/2018 3:06 PM
InfoSec Awareness

November’s Phishing Outreach Tip - Thanksgiving is getting us closer to a busy phishing season!

To: InfoSec Awareness

It’s worthy of repeating so please pay attention:

Get ready as we are heading into a busy phishing season!

Holidays like Halloween, Thanksgiving, Christmas, Hanukkah, Easter and Saint Patrick’s Day are popular times for criminals to launch phishing attacks. Scammers take advantage of the increased shopping and distractions to catch you off your guard.

Check out this example of a phishing simulation used last year resulting in a 28.18% click rate:

![Phishing Simulation](https://example.com/phishing_simulation.png)
Ven Invoice #0726188

Nick Young <nyoung@vencompany.com>
Helen Brown
Saturday 28 July 2018 at 10:27 p.m.
Show Details

I tried to reach you by phone but couldn’t get through.

Please get back to me ASAP with payment status of the invoice below.

Invoice #0726188
http://vencompany.payments.com/fhd_kkm23b3843/33804

Thank you,
Nick Young

---

I WILL FIND YOU
AND I WILL INTERVENTION YOU
• In general it's OK to open it, we don't count it.
• Hover with your mouse to get a preview of the url.
• We provide clues in the email.
• Attachments are more difficult but we can analyze them for you.
• You need to slow down.
What We Know

• Since 1/2018 no one has clicked more than 5 times on phishing exercises.

• We have had about 12 interviews of people clicking more than 5 times.

• We work hard to establish good rapport with our clients.
To: markalexander@westfieldgrp.com

Email Alert! Your entire emails are being forwarded from markalexander@westfieldgrp.com to a suspicious email: be*****@gmail.com with Signin details:

Country: Region: ##COUNTRY##
IP address: 23.31.54.18
Date: 5/27/2019
Platform: ##PC OS##
Browser: ##UNDETECTED##

We presume this may be a phishing attack by someone else.

Please verify

Check Mail Forwarding

Westfieldgrp.com IT Support
One Park Circle
P.O.Box 5001
Westfield Center, OH 44251
### Uptick In Phishing Reporting

<table>
<thead>
<tr>
<th>Date: Sunday</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Phishing</td>
<td>RE: [POTENTIAL PHISH]</td>
</tr>
<tr>
<td></td>
<td>Sun 6/9/2019 6:00 PM</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Date: Two Weeks Ago</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Phishing</td>
<td>RE: [POTENTIAL PHISH] Possible Westfield Insurance: VIN# WBAVD33506KV5827...</td>
</tr>
<tr>
<td></td>
<td>Thu 5/30/2019 6:04 PM</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Date: Last Month</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Phishing</td>
<td>RE: [POTENTIAL PHISH] Setting up a call</td>
</tr>
<tr>
<td></td>
<td>Wed 5/15/2019 2:24 PM</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Date: Older</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Phishing</td>
<td>RE: [POTENTIAL PHISH] Hi</td>
</tr>
<tr>
<td></td>
<td>Mon 4/15/2019 2:01 PM</td>
</tr>
</tbody>
</table>
What We Get Out Of It

Feedback on the program.

A better understanding of what people are having issues with in regards to identifying phish.

A sense of what is happening in people’s daily lives (in regards to their inboxes).

An opportunity to gain trust.
Hello,

I would like to set up a one-on-one consultation to make improvements with my emails. I suppose there is something I am unintentionally doing wrong and I would like to correct it. I do understand the potential impact these errors could make and I don’t want to do anything to jeopardize the company nor myself.

I look forward to hearing from you to set up a time.

Thank you.

Middle Market Underwriting Assistant