Staff Cybersecurity Awareness

Presented to AFNWA Employees
September 2023

Trevor Martin, IT Coordinator

How we plan on staying current with ongoing threats

The AFNWA conduct spear phishing campaigns to test and sharpen our staff's skills to identify these potential threats by using Cofense PhishMe Awareness.

These exercises provide a glimpse at current templates and messages that can bait people into getting infected by malware or ransomware and also provide educational material to those who may have potentially fallen victim to a tactic.

We encourage all staff to use the Report Phishing tool in your Outlook app on your laptop and phone to start an investigation.

How we plan on staying current with ongoing threats (cont'd)

The AFNWA IT team push critical and important updates to your laptops to ensure current exploits have been patches to reduce vulnerabilities vectors. It's important that staff load up their laptops every now and then allow the updates to take place and to call home so we can see the current missing updates.

Update mobile apps with Knox Management.

Report Phishing App – Outlook and Outlook Mobile

You can report a suspicious e-mail in Outlook by selecting the message you want to report and click on the Report Phishing button:

Triggering an investigation will create a ticket in helpdesk for the IT team to review the email and take action if required and advise the reporter how to proceed.

Cofense PhishMe Awareness Information

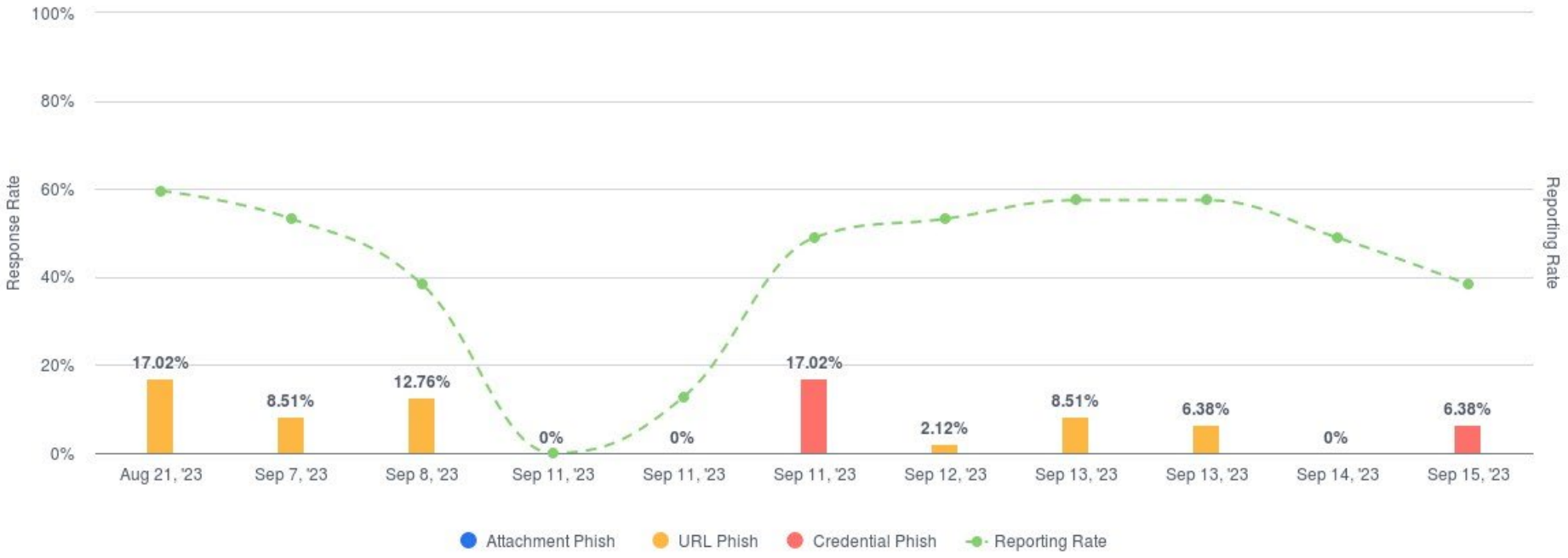
Information we can see as the awareness campaign facilitator:

- Who reported emails
- Who clicked on emails and didn’t report
- Who clicked on phishing links
- Who opened attachments
- How long users viewed education material
- Who input in their credentials in a phishing website

Cofense PhishMe Analytics

Overall Responses

Review response trends based on scenario types and reporting rate over the selected time period.



Recent Cyber Attacks on Critical Infrastructure and Institutes

- On Friday, February 5th, 2021, a hacker initiated an attack on an Oldsmar, Florida water treatment facility which briefly adjusted the levels of sodium hydroxide from 100 parts per million to 11,100 parts per million.
- On Saturday October 30, 2021, a cyberattack impacted IT systems supporting the delivery of healthcare services in Newfoundland and Labrador. An unauthorized third party accessed parts of the health care technology infrastructure, which resulted in an IT systems outage
- On November, 26, 2020, the municipal computer network in Saint John, N.B., had been dark for almost two weeks — taking down the city's website, costing the city thousands of hours in lost work and affecting its emergency dispatch system.

Oldsmar, Florida – WTF Attack

- Preliminary findings suggest the hacker used a dormant remote access software to access the system. That software was identified as Team Viewer.
- The incident highlights how some critical infrastructure systems are vulnerable to hacking because they are online and use remote access programs, sometimes with lax security.
- Later findings after infrastructure reviews with Cybersecurity exports suggested that the act may have been done by someone with previous knowledge of the system and still had access. There was no evidence supporting an outside threat from another state or nation.

Healthcare Services in NFLD, NL

- The report says the attacker successfully initiated a VPN connection to the environment managed by the Newfoundland and Labrador Centre for Health Information while using compromised credentials of a legitimate user account.
- Personal information of more than 58,000 people was compromised in the siege.
- Credentials were compromised via Phishing Email
- As of May 2020, the cyberattack costed the province $16million in damages.

City of St John, NB Ryuk Attack 2020

- Ransomware was initiated via an Excel document e-mailed to a city employee who opened the file and the ransomware began encrypting documents and computers.
- The city lost access to documents, emails and the emergency call center lost connectivity, their computer aided emergency services dispatch system and mapping tools.
- Ryuk is a ransomeware variant known to target large enterprises, hospitals and critical infrastructure and demand extremely large ransoms.
- The city of Saint John spent $400,000 of tax payers money to rebuild the network from scratch after insurance covered most of the $2.9million bill.

Wela'lin / Woliwon