Author: Cofense Intelligence

Wolves in Sheep's Clothing: Industry-Specific Targeted Phishing Attacks

Subject customization using either the recipient's name, email address, phone number, or company name is a common tactic used in phishing emails to deceive recipients. Threat actors often include the company name or designated recipient's personal information to disguise the true intent of the email. Our analysis shows that certain industries are more targeted by these types of attacks than others. From data drawn from Q3 2023 to Q3 2024, Cofense Intelligence identified the top five targeted industries and the common subject customization tactics that were seen within each industry.

Cofense Intelligence utilizes redaction to safeguard our customers' personally identifiable information (PII) and proprietary company information. To counter the personal information included within the subject, Cofense Intelligence meticulously redacts such information to protect our clients. This approach allows us to maintain privacy while continuing to deliver accurate and actionable intelligence to our customers via ThreatHQ while still making use of Cofense's large customer base. The redaction progress is integral to our commitment to protecting customer privacy, as it allows us to provide clients with clear actionable intelligence without exposing sensitive information.

Top Five Targeted Industries

The top five most-targeted industries where subject redaction was required includes finance and insurance, manufacturing, mining quarrying oil and gas extraction, healthcare and social assistance, and retail trade. Cofense Intelligence also identified a relationship between email themes and threat actors using subject customization as a tactic, quarterly volume fluctuations within each industry, and unique subject-redacted samples.

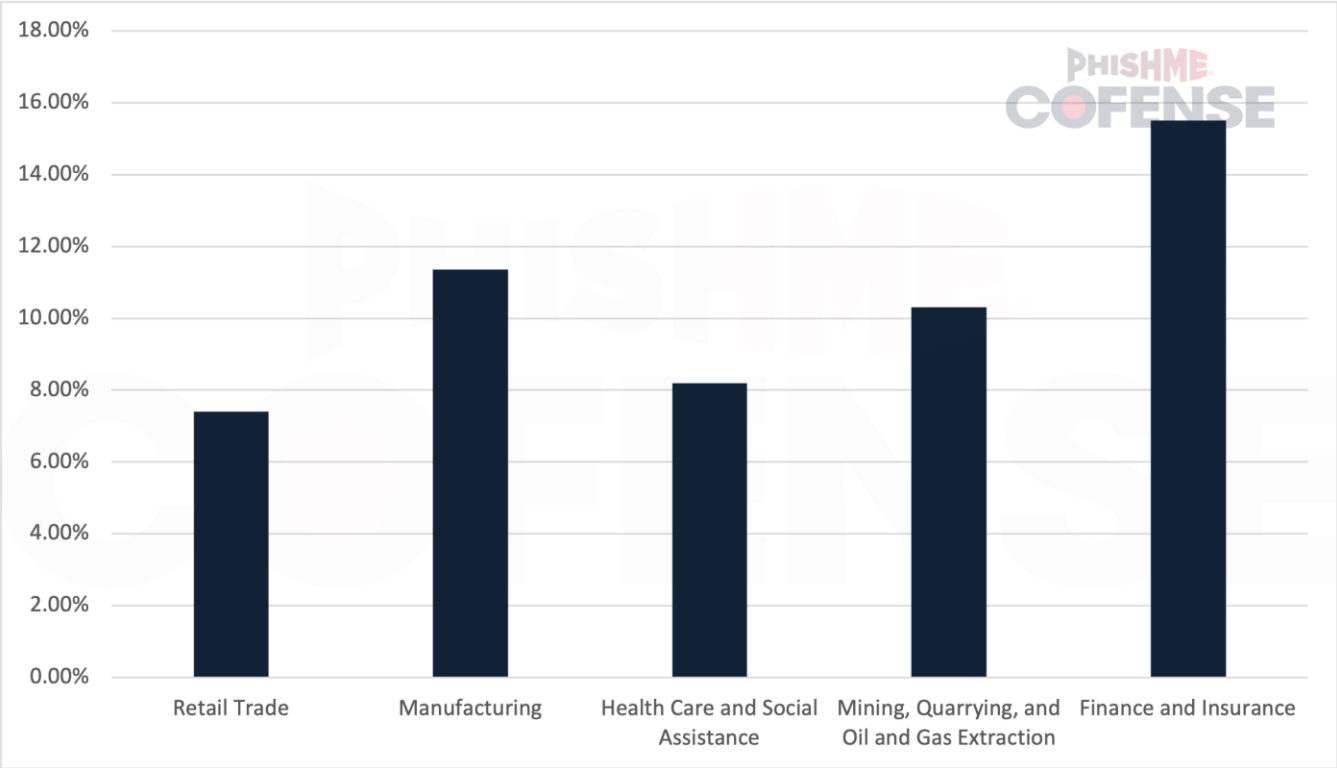

Figure 1: Top five industries targeted by emails with customized subjects requiring redaction.

Finance and Insurance

Finance and insurance is the top-targeted industry to receive emails delivering credential phishing with customized subjects. In 15.5% of all credential phishing emails where information needed to be redacted from the subject, the recipient was listed under the finance and insurance industry. The types of subject lines observed in attacks targeting this industry often mimic business communication such as invoices, business documentation, and forms requiring attention. The finance and insurance industry saw the highest number of subjects requiring redaction in July 2023 and the lowest in December 2023. Although volumes increased towards the end of Q3 2024, the average volume of each quarter in 2024 is still significantly lower than the highest in Q3 2023.

Table 1: Examples of customized subjects sent to finance and insurance customers.

Selected Subjects
<recipient name or identifiable information> shared "Invoice20248904.pdf" with you
Invoice from <recipient name or identifiable information>
ACH on 2024-06-28 For <recipient name or identifiable information>¬† REF: PAY-SB-202213 via <recipient name or identifiable information>
(NDA-Adjustment) Working Group List for <recipient name or identifiable information>

Manufacturing

Manufacturing is a highly targeted industry when it comes to the inclusion of PII within the subject of emails. Cofense Intelligence has seen that in 11.3% of all emails where subject redaction took place, the recipient's industry was classified as manufacturing. This tactic has proven to be particularly effective in the manufacturing industry where email communication around orders, contracts, and agreements are common. By personalizing these subject lines, threat actors can create a sense of legitimacy, increasing the likelihood of recipients engaging with malicious content. Additionally, since contract and order-based communication are often expected within this industry, these emails tend to blend into regular business operations making them harder to detect. Much like the finance and insurance industry, the manufacturing industry saw the highest volume of emails containing personalized subject lines in Q3 2023. Overall volumes of emails with subjects requiring redaction that target the manufacturing industry have continued to trend downwards, with Q3 2024 having only 24% of the volume of Q3 2023.

Table 2: Examples of subjects sent to manufacturing customers.

Selected Subjects
Proposals from <recipient name or identifiable information>
File Shared By <recipient name or identifiable information>¬† On Behalf Of <recipient name or identifiable information>
NEW P.O. # 94153 from <recipient name or identifiable information>
New Update: Employee Assistance Program (EAP) Timesheet Report: Action Required on <recipient n

Mining, Quarrying, and Oil and Gas Extraction

The mining, quarrying, and oil and gas extraction industry is also highly targeted by emails with customized subjects. In 10.3% of all emails where information needed to be redacted from the subject, the recipient was listed under the mining, quarrying, and oil and gas extraction industry. The common subject lines requiring redaction were based on proposals, invoices, and notifications for shared documents. Like the finance and insurance and manufacturing industries, the mining, quarrying, and oil and gas extraction industry saw the highest volume of subjects requiring redaction in Q3 2023. Again, this was a gradual decline; however, the decline was much less pronounced for this industry.

Table 3: Examples of subjects sent to mining, quarrying, and oil and gas extraction customers.

Selected Subjects
Contract Proposal for service - <recipient name or identifiable information>
Document shared with you: #<recipient name or identifiable information> _Financ.....#88456.docx

Selected Subjects
FW: New Invoice Acknowledgement 6472749IK From <recipient name or identifiable information>
(<recipient name or identifiable information> - shared "Quotation_Request20234328P (signed).pdf" with you

Health Care and Social Assistance

Threat actors often target the healthcare and social assistance industry when including PII within the subject of an email. Across all emails where subject redaction took place, 8.2% of the emails were targeted to a customer within the healthcare and social assistance industry. Examples of the types of subjects that Cofense Intelligence sees for these emails include notification-based or document-related emails. This is an efficient tactic within the hospital industry as it is usual for medical industries to receive document-based emails throughout their daily tasks. Like the other industries, the healthcare and social assistance industry saw the highest volume of credential phishing emails with subjects requiring redaction in Q3 2023. In this industry, Q4 2023 saw the lowest volume of all observed quarters, breaking the previous trend of a gradual decline. Q1 and Q2 2024 remained consistent with only a slight dip in Q3 2024.

Table 4: Examples of subjects sent to healthcare and social assistance customers.

Selected Subjects
Hi <recipient name or identifiable information>¬†Please Sign :<recipient name or identifiable information> Agreement.pdf
<recipient name or identifiable information>: Approved Benefits Payroll Increase on September 25, 2024 drPLE
FW: <recipient name or identifiable information> [ACTION NEEDED]
Documents Accomplished: Please Sign & Return Swiftly via e-Sign via <recipient name or identifiable information> DOC-984787

Retail Trade

Retail trade is another commonly targeted industry where PII is included within the subject of the email. In 7.4% of the emails where subject redaction was required, the recipient's industry was listed under the retail trade industry. Examples of the types of subjects that Cofense Intelligence sees for these emails include subjects related to sales, contracts, and urgent shipments to make the email look as if it is a legitimate business interaction Just like with the other top five industries, the retail trade industry saw the highest volume of credential phishing emails with customized subjects requiring redaction in Q3 2023. However, rather than a gradual decline, volumes increased from Q4 2023 to Q3 2024. In fact, Q3 2024 volumes were 77% of Q3 2023, indicating that Q4 2024 might see a return to previous levels.

Table 5: Examples of subjects sent to retail trade customers.

Selected Subjects
Update for All <recipient name or identifiable information> Employees
<recipient name or identifiable information> Contract - Final for <recipient name or identifiable information>
<recipient name or identifiable information>Has shared a Contract Project.
Email Service Request - Action Alert for <recipient name or identifiable information>

Connection between Theme and Redacted PII

Cofense Intelligence observed a correlation between the theme and redacted PII from emails. Voicemail-themed emails tend to contain the recipient's personal or company name within the subject of the email and the .HTM(L) attachment(s) names. An example of when both a subject and attachment name are redacted would be ATR 378550 where the subject is "Call_Service-PlayBack- <recipient name or identifiable information> 1b57bf998dea7cf4d8cb7d2cd1719cf7eddf2e9e" and the attachment is" <recipient name or identifiable information>_VM-Now<recipient name or identifiable information>VM.html". Although .HTM(L) files are not commonly utilized within organizations for legitimate use, attackers continue to utilize them in their credential phishing attempts.

Another example of the correlation between theme and redacted PII can be observed with finance-themed emails. The email subject is often an ACH or remittance-based subject followed by the recipient's name or company name while including a .DOC(X) attachment with PII included in the file name. An example of this occurring would be ATR 376731 where the subject is "Funding/EFT Remittance For <recipient name or identifiable information>-EFT-01uxw" and the attachment is "<recipient name or identifiable information>-Invoices.docx". This makes the email appear as legitimate as it personalizes both the subject and attachment of the email.

Top-Delivered Attachment Type on Subject Redacted Emails

Our analysis reveals that the most frequently encountered malicious file types from credential phishing-based emails are .HTM(L) and .DOC(X) files. This aligns with the prevalent formats used for legitimate documents in daily operations across industries such as contracts, invoices, and reports. Many of the email subjects contain words that are in-line with routine communications, which further increases the probability of employees interacting with these emails.

.HTM and .HTML Attachments

.HTML and .HTM are the most common file extensions on attachments for credential phishing emails that have subjects requiring redaction. Hypertext Markup Language (HTML) files are a file format that is generally used to

display what appears to be a standalone webpage. For the emails that contain a redacted subject that has attachments, Cofense Intelligence observed that 90.3% of these emails have the .HTM or .HTML file extension. This seems to be due to the efficiency of HTML pages being able to replicate legitimate login pages. Often the HTML page will have the recipient's email address embedded in it. Using this embedded email address to populate the credential phishing page displayed by the HTML file with the email address portion of the login screen already filled out with the recipient's email address increases the chances of the user falling prey to the HTML file as it closely replicates a legitimate login page.

.DOC and .DOCX Attachments

Attachments with the .DOC or .DOCX file extension being attached to credential phishing emails with subjects requiring redaction are relatively common, although significantly less common than .HTM(L) files. Cofense Intelligence observed that 9.4% percent of the credential phishing emails with subjects that required redaction had a .DOC(X) file attached. Threat actors generally will embed malicious URLs or QR codes into the .DOC(X) files. These links will direct the users to phishing sites designated to capture login credentials. .DOC(X) files are often allowed past secure email gateways (SEGs) due to the common usage in business environments.

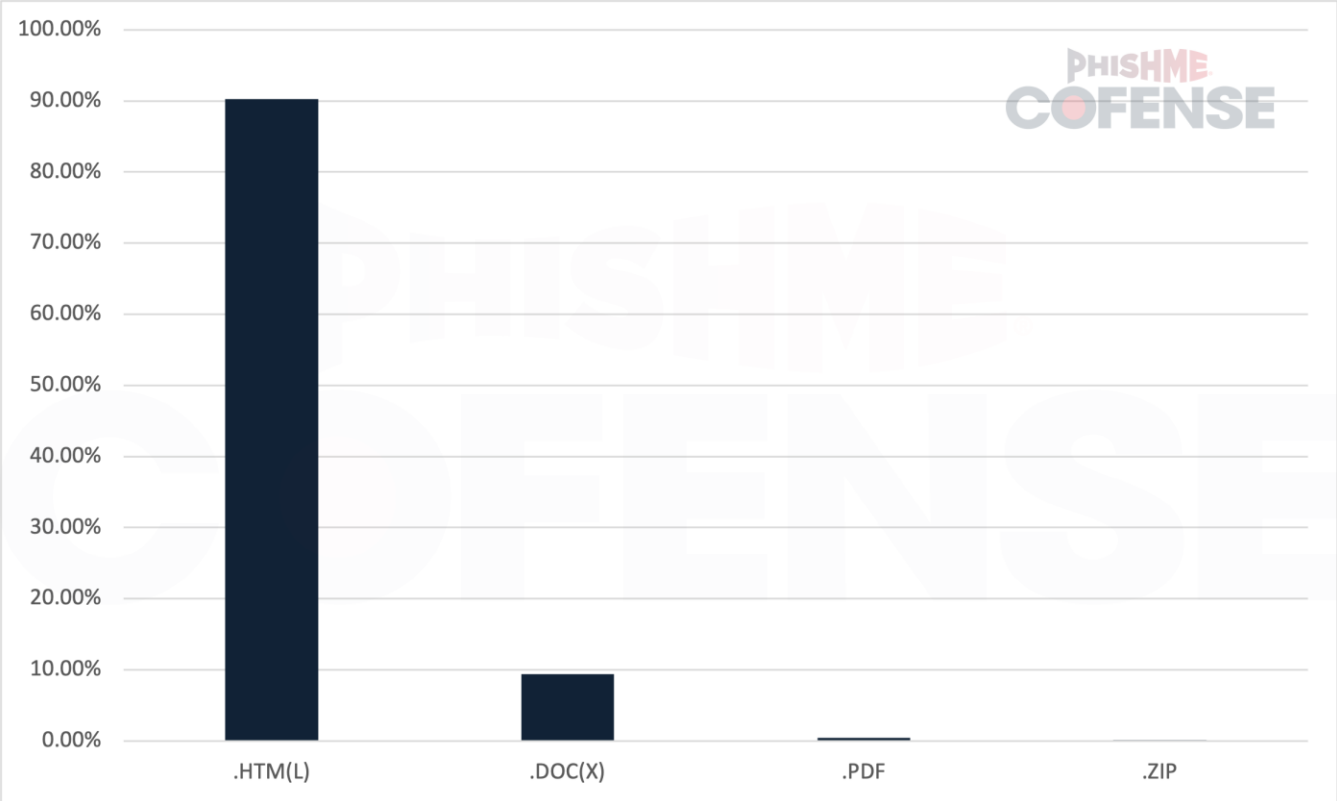

Figure 2: Top attachment extensions for credential phishing emails with subjects requiring redaction.