Year-End Phishing Lures: Fake Raises, Q4 Invoices, and Access Reviews

By Ivan Khamenka

Published: 2026-10-22 · Archived: 2026-11-23 02:00:25 UTC

Types of year-end lures observed

Compensation and salary adjustments

Compensation-related messages provide a strong incentive for employees to interact, particularly when they appear to contain information about annual reviews, salary changes, or upcoming payroll adjustments.

Netcraft identified several phishing emails presenting recipients with a “2026 Compensation Adjustment Letter” document. The message claimed to contain results of annual compensation reviews and displayed supposed salary increases, referenced upcoming payroll cycles, and instructed recipients to scan QR codes to review the signed documents.

The same underlying template was observed targeting multiple organizations, with company names, recipient information, and QR codes changed while the compensation language and document structure remained the same.

Figure 1: Personalized compensation adjustment lure presenting an annual salary increase and QR code-based document review workflow.

Other examples did not include a QR code but instead requested that recipients download a document from the email. In these examples, it appears the email was sent through Google's SMTP relay infrastructure using intime[.]cz. The email contained no actual PDF attachment. Instead, the “Review” button redirected to hxxps://bvlbetonvloeren[.]be, which returned a “404 Page not found” error at the time of writing.

Figure 2: Generic salary increase PDF identified mentioning several different organizations.

In another example, Netcraft identified a compensation and payroll-themed phishing email that claimed employees could review staff salary information, performance awards, attendance data, and a final income-tax spreadsheet. The message presented a fake Excel workbook and redirected recipients to an external domain, englaus[.]sbs.

The landing page continued the document-access theme by impersonating a SharePoint-style portal and presenting supposed financial and staff salary content, including a “Receipt” section and a “Staff Salary and Performance” gallery. Selecting the content led to a separate “Secure Document Access” prompt requesting an email address and password before the document could supposedly be viewed.

Figure 3: Fake SharePoint-style document portal prompting the recipient to enter their email address and password to access supposed salary and performance documents.

Netcraft also observed a SharePoint-themed lure claiming that a “September Bonus Payment.pdf” had been shared with the recipient. The email stated that the bonus payment was available for review and acknowledgement and used a personalized shared-document notification to make the request resemble a routine HR workflow.

Figure 4: SharePoint-themed phishing email claiming that a “September Bonus Payment.pdf” document had been shared with the recipient for review and acknowledgement.

Rather than linking to legitimate Microsoft or SharePoint infrastructure, the “Open” button redirected recipients to content hosted on Google Cloud Storage. The landing page displayed a blurred financial document in the background and a fake “Secure Excel Download” authentication prompt. Recipients were asked to enter an email address and password before they could supposedly download the file.

Figure 5: Fake secure Excel download page displaying a blurred financial document and prompting the recipient to enter credentials before accessing the supposed bonus-related file.

The use of a blurred document preview reinforced the impression that a legitimate financial record was waiting behind the authentication prompt, while the “Authentication failed” message mimicking an SSO error encouraged the recipient to provide credentials again.

This activity was not isolated to a single recipient or organization. Netcraft observed the same SharePoint-themed lure distributed across numerous organizations, with each message using the same blurred document preview and the same underlying URL while changing the organization and recipient details.

The broader campaign also appeared to span multiple sectors, including aviation, telecommunications, industrial manufacturing, real estate, technology, and financial services, suggesting the lure was designed for reuse rather than a single vertical. Several organizations appeared to be targeted repeatedly, and a noticeable number of the names were associated with the Middle East, indicating a possible regional concentration within an otherwise broad payroll and compensation-themed campaign.

Q4 financial and budget documents

Netcraft identified a phishing email impersonating the cloud-based document-sharing and signing platform Docusign with lures themed around Q4 financial documents. The message claimed that recipients needed to review and sign a “Q4 2026 Statement of Account” and “Q4 2026 Budget Analysis,” presenting the files as a PDF and spreadsheet awaiting signature.

Although the email used Docusign branding and document-signing language, it did not appear to be sent through Docusign infrastructure. Instead, the message was sent from unrelated infrastructure, and the embedded links redirected to third-party domains rather than Docusign-controlled services. The message also used an explicit signing deadline and a document expiration date to create urgency.

Figure 6: Docusign-themed phishing email presenting a Q4 2026 Statement of Account and Budget Analysis as documents awaiting the recipient's signature.

Access reviews and recertification

Year-end administrative activity also extends beyond HR and Finance. IT and security teams may conduct access reviews, entitlement recertification, privileged-access reviews, or policy attestations. Attackers can also abuse that terminology.

Netcraft identified another Docusign-themed phishing message using an “Access Review” pretext, with the subject “ATTN – Access Review Msg REF ID_PO ORD.” The email claimed that a new document required the recipient's signature and presented a “VIEW DOCUMENT” button, while also using familiar Docusign-style language such as “Do Not Share This Email” and references to a secure Docusign link to make the message appear more convincing.

The access-review theme mirrors the kind of access recertification, entitlement review, and policy acknowledgement workflows organizations may carry out on an annual or quarterly basis. Framing the request as a document awaiting signature adds urgency while still resembling a routine compliance or administrative task.

The embedded link ultimately directed the recipient through third-party redirect infrastructure to an unrelated login domain rather than legitimate Docusign infrastructure. The sender also claimed to be dse_NA3@docusign.net, but the message was received directly from 151.244.232.50 rather than infrastructure associated with Docusign. This mismatch between the claimed sender and the actual sending host suggests the sender identity was spoofed or otherwise unauthorized.

Figure 7: Docusign-themed access review phishing email prompting the recipient to view and sign a document through a fraudulent “VIEW DOCUMENT” link.

Invoices and financial close

Some year-end social engineering does not need to rely solely on a fake login page or credential theft. Accounting, invoice, and protected-message lures can also be used to create a believable pretext for obtaining sensitive business documents directly from employees.

In one example, Netcraft identified a message styled as a Microsoft 365 encrypted email from “Accounting,” with the subject “Invoice Follow-Up.” The email claimed the recipient had received a protected message relating to “Outstanding Invoices” and instructed them to open it using a verification code.

Themes like accounting, overdue invoices, and protected financial communications can appear especially legitimate during busy end-of-quarter or year-end periods, when staff may already expect invoice reviews, reconciliations, and payment-related follow-up.

Figure 8: Microsoft 365-themed “Invoice Follow-Up” lure presenting a protected message related to outstanding invoices and prompting the recipient to open the document using a verification code.

Lures like this do not just present the risk of credential theft. The same type of social engineering pretext could also be used to persuade a recipient to send, upload, or share sensitive documents, such as outstanding invoice reports, account reconciliations, budget workbooks, Q4 forecasts, payroll records, tax documentation, vendor banking details, or other internal finance materials.

In these scenarios, sensitive information itself may be the primary target. A successful attack could therefore result in unauthorized disclosure of internal financial data even without a final malware payload or stolen credentials. Depending on the jurisdiction and industry, this could also trigger regulatory reporting obligations.

Annual statements and benefits

Netcraft also observed recurring phishing emails impersonating the U.S. Social Security Administration (SSA) and encouraging recipients to access a supposed 2026 Social Security statement. The message described the document as an official “proof of income” or “benefit letter” and urged recipients to review their earnings and benefit information, while warning that delayed access could result in missed deadlines or service interruptions.

Although the email did not explicitly reference year-end activity, the use of a current-year statement and financial review language gives the lure an annual administrative context that may appear increasingly plausible as the year progresses.

The message used seemingly legitimate SSA branding, including an image loaded from ssa.gov, but the “VIEW YOUR 2026 STATEMENT” button did not lead to an SSA-controlled destination. Instead, the link redirected through medium[.]com before pointing to rsfashionsdesignbd[.]com.

The message was sent from tropical100[.]com.do infrastructure and included a DKIM signature for that domain rather than SSA, reinforcing that the apparent government branding was unrelated to the actual sender. This example shows how attackers can combine trusted visual assets, annual financial themes, and redirect services to make an otherwise unrelated email appear legitimate.

Figure 9: Social Security Administration-themed phishing email encouraging the recipient to access a supposed 2026 benefits statement while warning of missed deadlines or service interruptions.

Generic protected and shared documents

Generic document lures can be effective because the message does not need to explain exactly what the recipient is being asked to access. Phrases such as “protected message,” “shared document,” “requested file,” or “secure document” can be paired with a realistic subject line that supplies just enough context, such as a bonus payment, access review, invoice follow-up, budget document, or annual statement.

The landing page can remain largely unchanged while the email subject, sender name, document title, and impersonated department are adjusted to suit different organizations and recipients. This makes the same underlying phishing template reusable across HR, Finance, IT, procurement, and executive workflows.

The time of year can provide additional credibility and urgency even when neither the email nor the landing page explicitly mentions year end. During periods of financial close, annual reviews, benefits administration, budget planning, and access recertification, employees may already expect more document-sharing notifications and requests from teams and third parties that they interact with less frequently.

A generic message that might appear unusual during a quieter period may therefore blend into legitimate business activity when it arrives alongside real deadlines and increased administrative pressure. In these cases, the seasonal element exists primarily in the timing and surrounding business context rather than in overt end-of-year language.

Recommendations

Organizations should treat year-end phishing as a contextual risk rather than relying only on explicit seasonal keywords. Employees should be encouraged to verify unexpected document-sharing, signature, payment, and access-review requests through a known communication channel, particularly when the message leads to unfamiliar infrastructure, requests credentials, asks the recipient to scan a QR code, or prompts them to upload internal documents.

Security teams should also monitor for combinations of business-process language and requested actions, while establishing clear, predictable workflows for legitimate HR, Finance, and IT communications. These measures can help reduce both account compromise and the unauthorized disclosure of sensitive budgets, payroll data, invoices, forecasts, and other internal documents.

Source: https://www.netcraft.com/blog/year-end-phishing-lures-fake-raises-q4-invoices-and-access-reviews