# Attachments



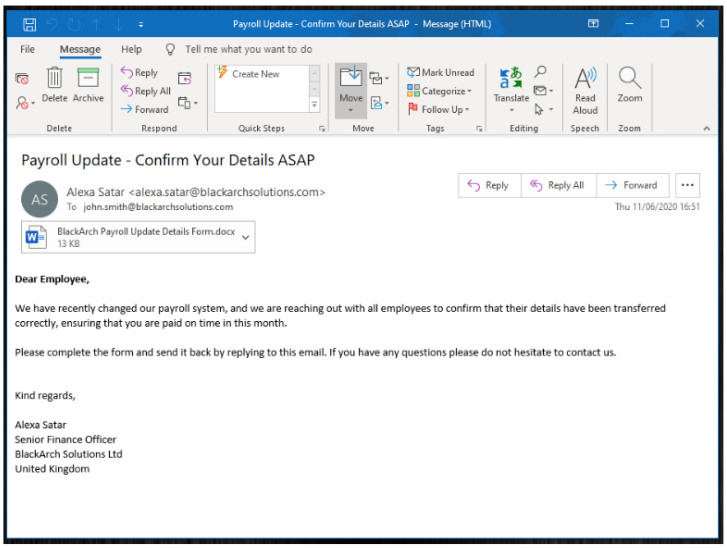

As mentioned in the lesson on **Malicious Files** in **PA2) Types of Phishing Emails**, malware can be distributed through email attachments, such as Microsoft Office documents that are utilizing malicious macros to download malware to the target system. In phishing campaigns, we will typically see three categories of attachments:

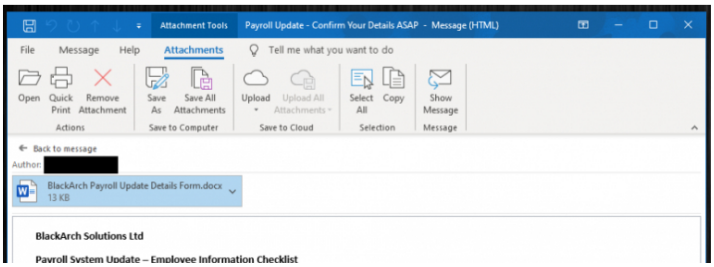
- **Non-malicious files that are used for social engineering** (such as invoices, letters of appeal, and images)
- **Non-malicious files that have malicious hyperlinks** (such as PDFs that contain a link to a malicious site)
- **Malicious files** (such as malicious scripts, or more likely Microsoft Office documents with malicious macros, such as Word or Excel)

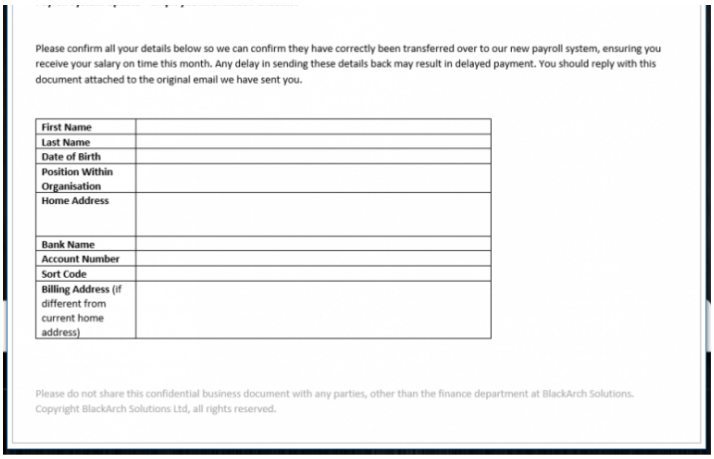
We will cover examples of each of these below to further your understanding of how attackers can utilize attachments to bypass security controls and successfully phish users.

## SOCIAL ENGINEERING FILES

If an attacker is posing as a member of the Human Resources department at the target organization, they could try to extract information from a legitimate employee by sending them a form as an attachment that they need to fill out to assist with a payroll system change or any other bogus pretext scenario. This can work well with other tactics such as sender spoofing to make the sending address look like it's actually coming from the HR department of the organization. The below example is playing on social engineering principles such as urgency, stating that if the employee isn't quick, they might not get their salary this month, in an effort to rush them, giving the target less time to think about what they're being asked to do.





Please confirm all your details below so we can confirm they have correctly been transferred over to our new payroll system, ensuring you receive your salary on time this month. Any delay in sending these details back may result in delayed payment. You should reply with this document attached to the original email we have sent you.

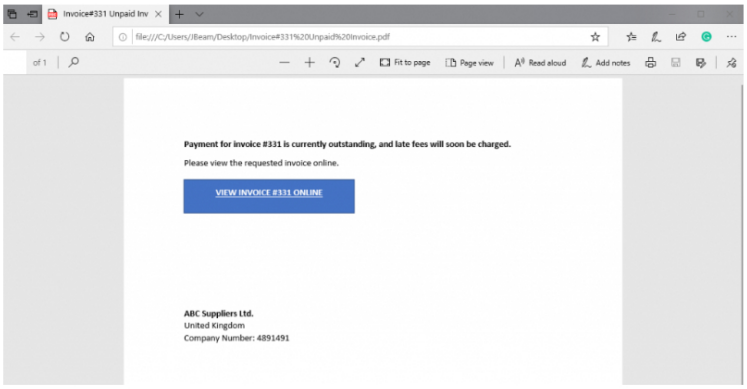
| | |
|---|---|
| **First Name** | |
| **Last Name** | |
| **Date of Birth** | |
| **Position Within Organisation** | |
| **Home Address** | |
| **Bank Name** | |
| **Account Number** | |
| **Sort Code** | |
| **Billing Address** (if different from current home address) | |

Please do not share this confidential business document with any parties, other than the finance department at BlackArch Solutions.


This information might seem fairly harmless to give out, but this can be used to commit online fraud, blackmail, or further social engineering attacks where the malicious actor can pose as the target with more confidence if they have more personal information on them.

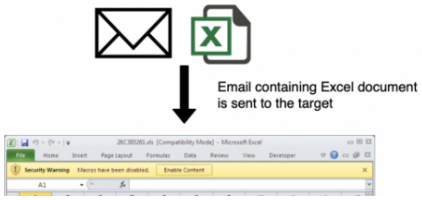
## LURE DOCUMENTS

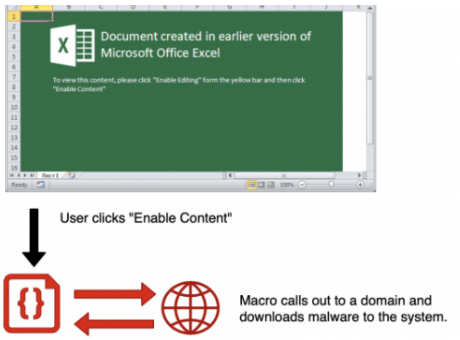
Inserting hyperlinks into a malicious email is common, and can potentially be detected easily by email security tools that retrieve URLs and sandbox them to see if the destination is malicious or has a bad community reputation. A way to prevent this is by including the hyperlink in a document, such as a PDF or Microsoft Word file. This means that the attachment itself isn't inherently malicious, but the hyperlink inside can be. In the below example, this file is a lure document to direct users to "view an invoice online". The destination URL could simply take the user to a malicious domain that downloads malware to the system.




## MALICIOUS FILES

The most common form of inherently malicious files are Microsoft Office documents that are utilizing macros to run malicious code on the system that opens the document. They can download additional malware to the system by reaching out to domains on the internet and retrieving files, then executing them. As mentioned in the **Malicious Files** lesson of the previous section, macros are now disabled by default, so the attacker needs to convince the recipient to click "Enable Content," allowing the macros to run. This diagram should be familiar, but it's good to show it again here.






Previous Topic
Back to Lesson
Next Topic