Common Types of Recent Phishing Emails to Look out For

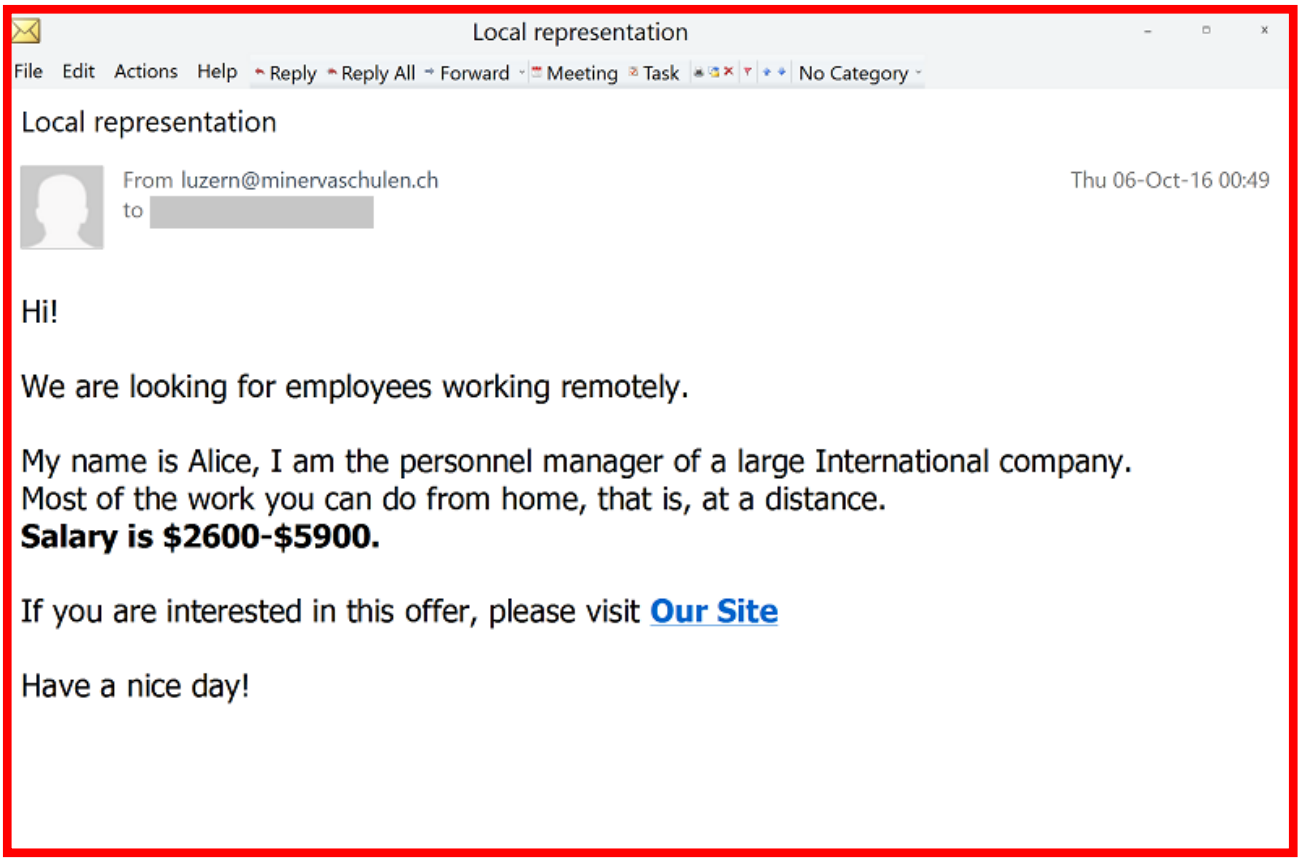
The present-day cybercriminals often opt for social engineering to achieve their malevolent goals. The reason is obvious – it turns out that manipulating humans is just as effective as exploiting code vulnerabilities to hack into computer systems. Plus, it's a no-brainer. All it takes is tailoring a trustworthy-looking email and sending it out to as many users as possible. By opening the attached files or clicking on embedded links, gullible recipients run the risk of catching viruses or exposing their online identity to theft.

Referred to as phishing, this technique is heavily used to distribute crypto ransomware that holds one's files hostage and demands a ransom for decryption. Another possible objective is to dupe people into willingly handing over their sensitive information, including passwords and credit card details, via rogue login pages.

Below is a list of the recent phishing email variants that users are most likely to encounter these days.

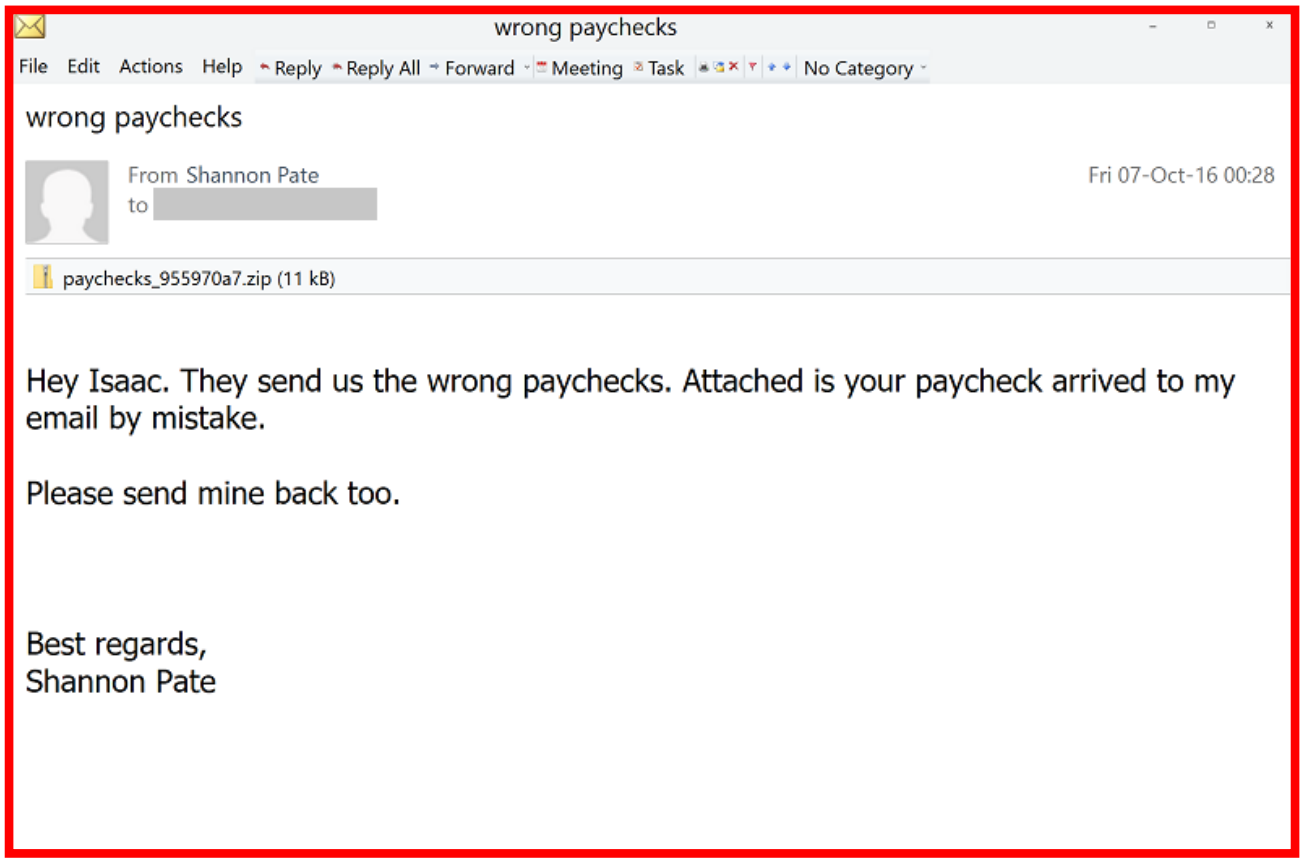
Job offer

When an enticing offer to work remotely for some "international company" shows up in your inbox, think twice before downloading attached files or clicking any links in it. These deceptive messages contain the salary size in bold font and deliberately provide very few additional details in order to encourage the user to visit a linked-to rogue landing page for more information.



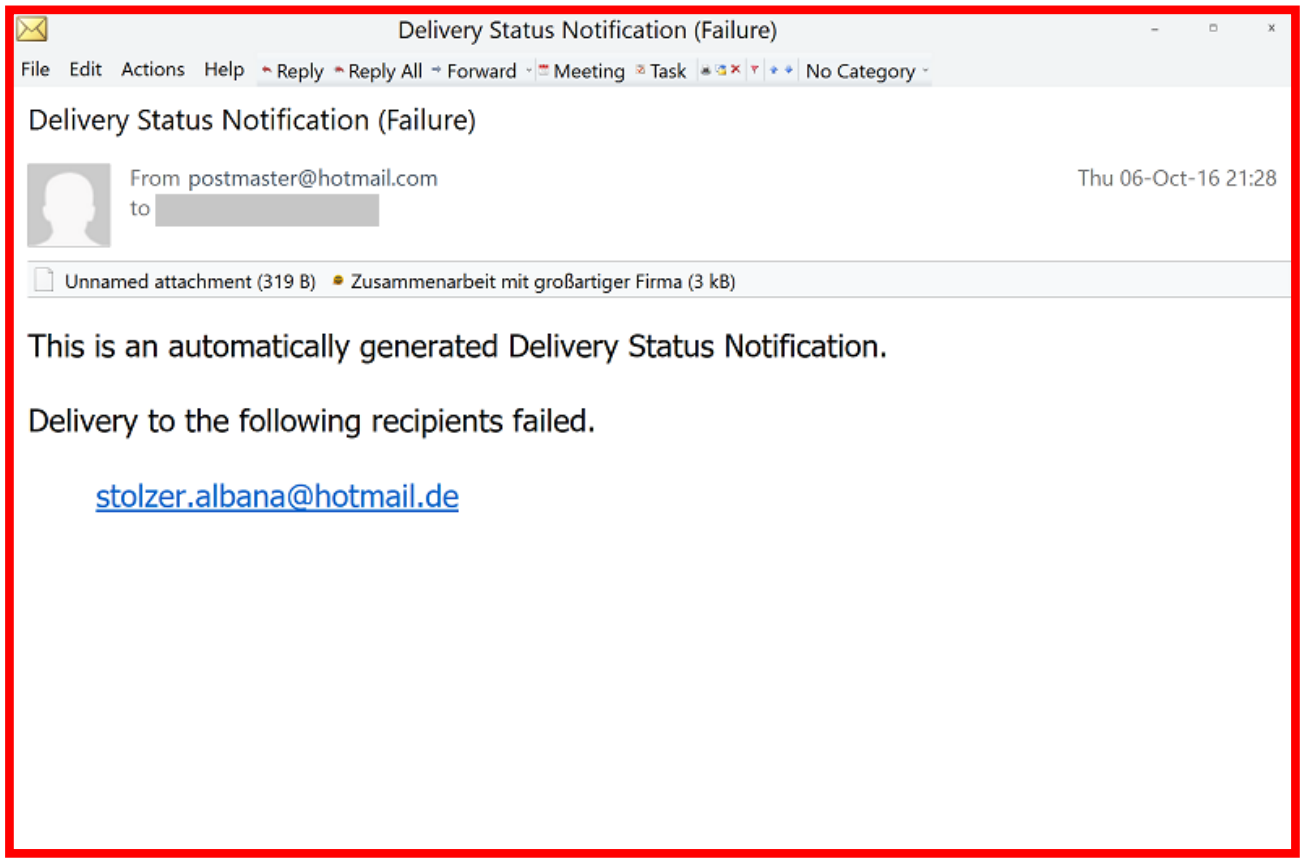
Wrong paychecks

Some phishing emails deliver a malicious file disguised as a paycheck. Even if the sender is unfamiliar, some people end up opening the attached document out of curiosity. Doing so is a bad idea. These are mainly ZIP archives that contain a harmful JS (JavaScript) file. Once opened, this object will instantly execute ransomware on the computer.



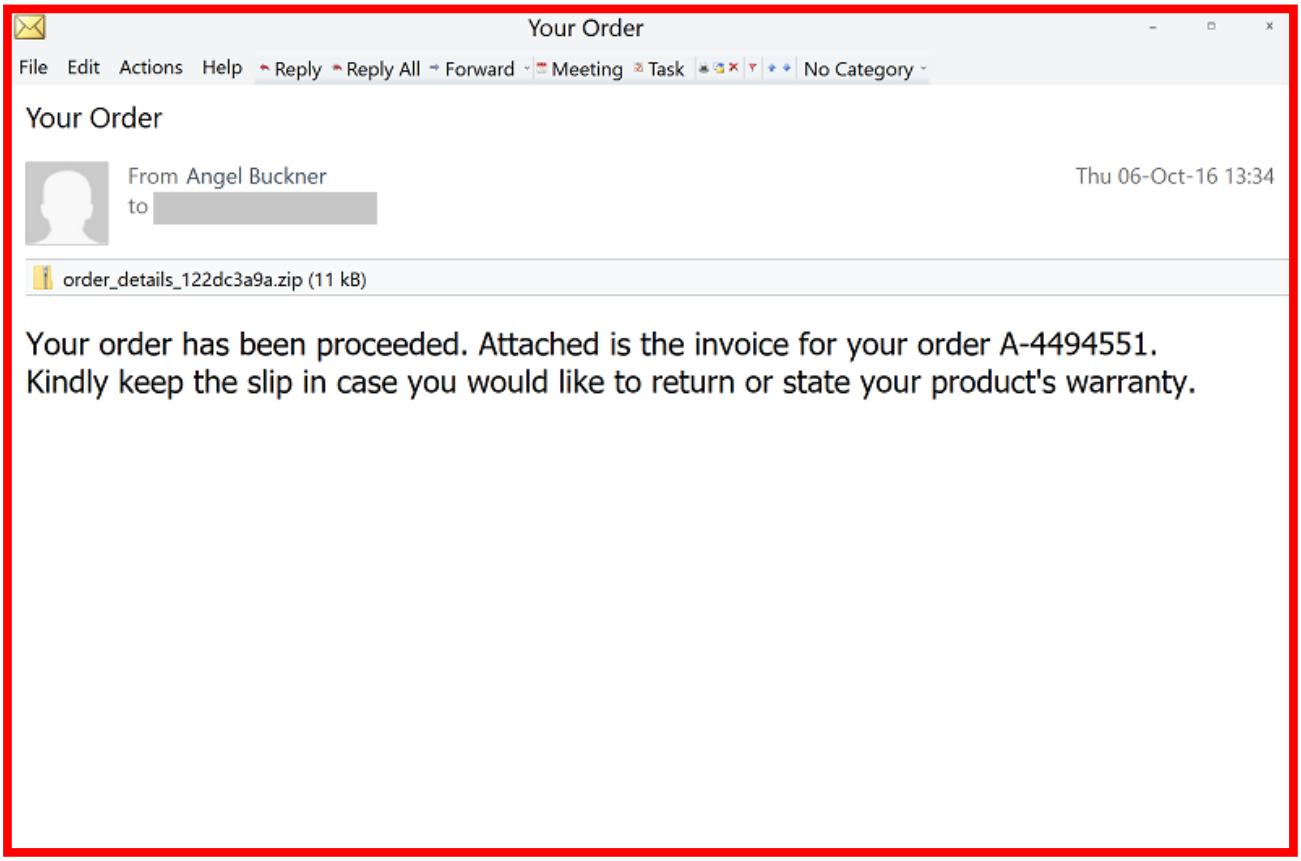
Failed delivery

Typically titled “Delivery Status Notification (Failure)” these phishing emails pretend to be generated automatically to inform a user about unsuccessful delivery of some message. They will contain the alleged recipient’s email address and one or several attached files. Again, if you happen to open the attachment, a piece of ransomware will attack your PC.



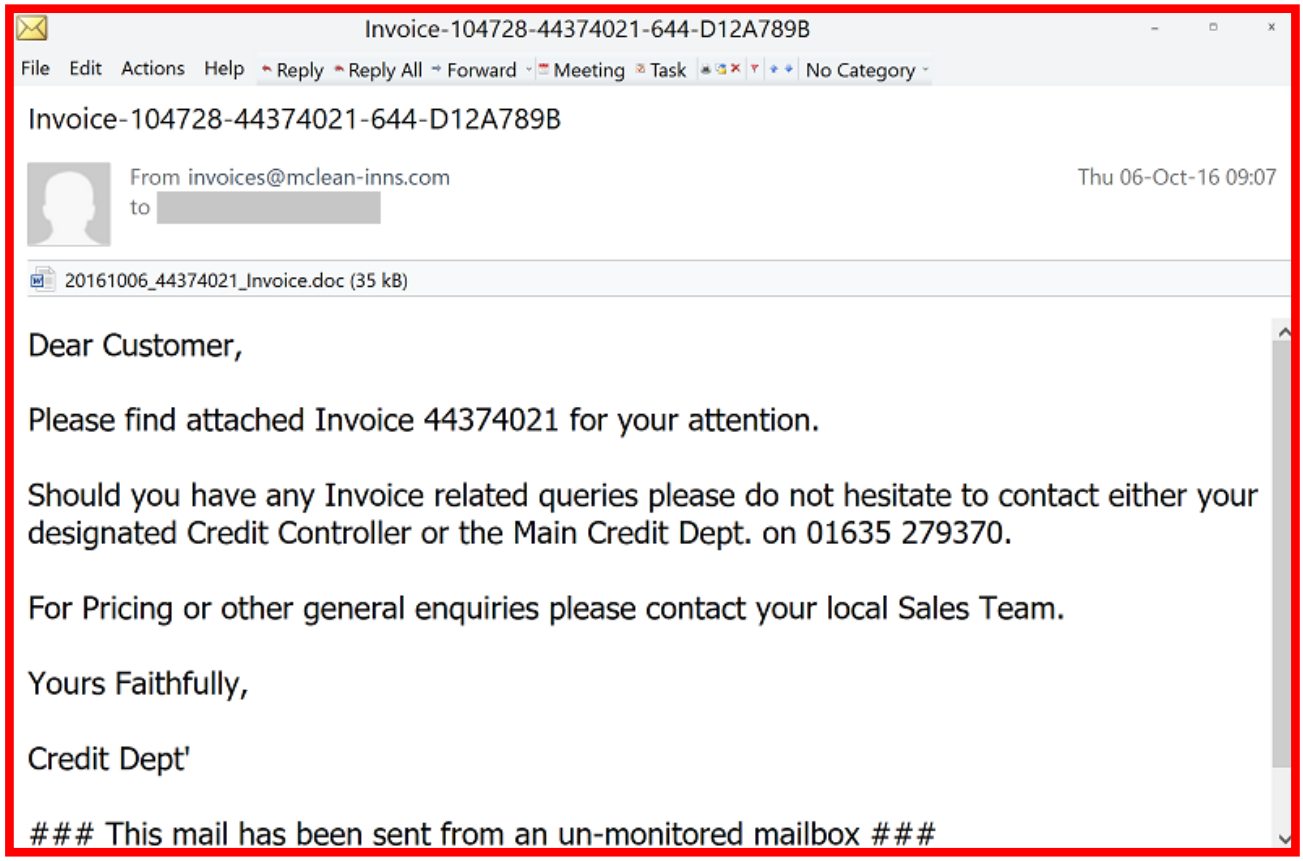
Order details

With the rise and ubiquity of ecommerce, people have gotten used to order notifications sent over email. Cybercrooks take advantage of this by sending rogue order details to potential victims. The wording of these phishing emails usually includes a warranty reminder and, most importantly, a reference to an attached file that you should never open unless you want to fall victim to ransomware.



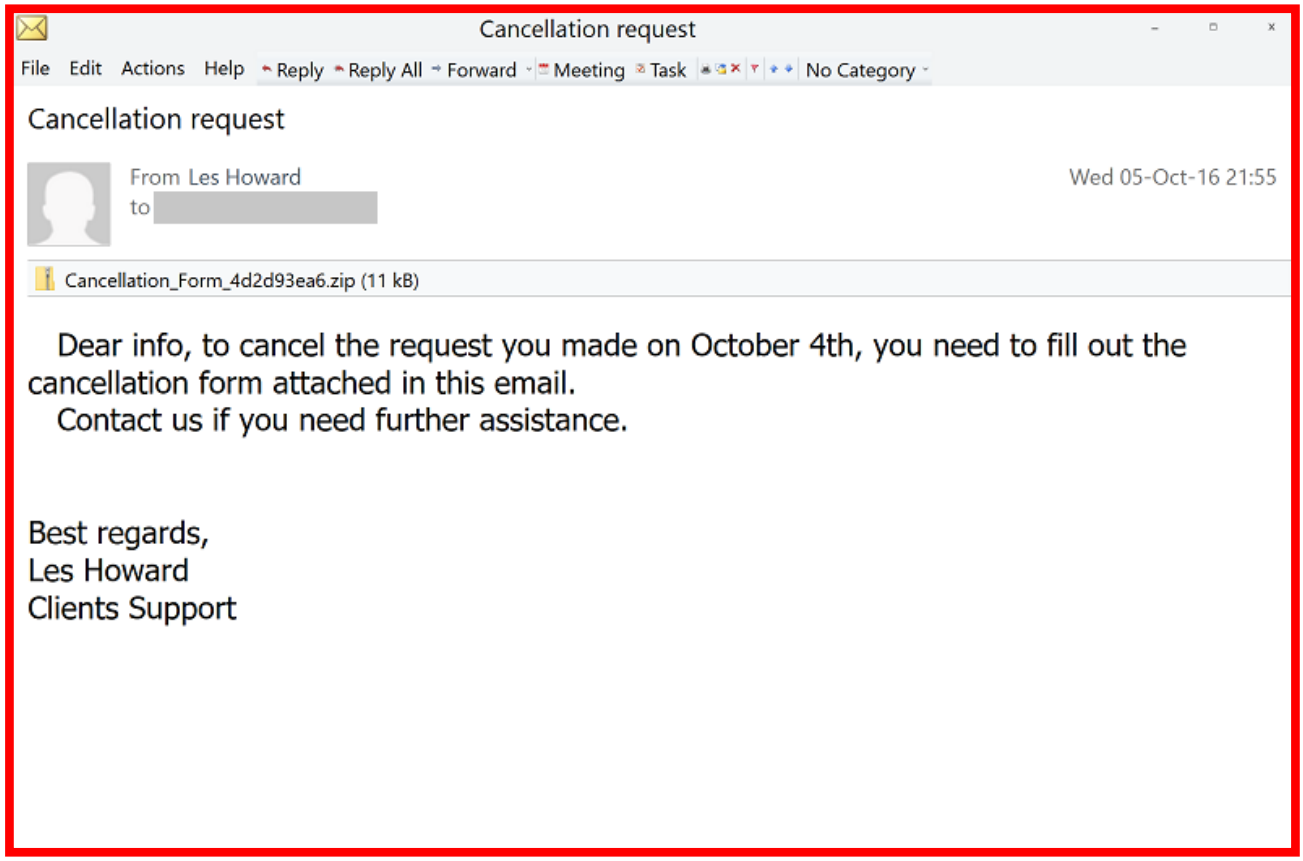
Invoice

This is one of the most widespread types, because emails with invoice-related subjects are catchy by their essence. The threat actors who distribute the newest Odin edition of the Locky ransomware use this tactic a lot. The attached Microsoft Word file named "[random_digits]_Invoice.doc" displays a prompt to enable macros, which are then exploited to deposit the crypto threat onto the PC.



Cancellation request

This phishing technique is aimed at persuading a recipient to open a booby-trapped cancellation form inside a ZIP archive. To make these emails more true-to-life, the fraudsters provide additional details, including the date that the purported cancellation request was made.



If you receive one of the above phishing emails, do not open the attachments or click on links inside them. In case you already did and thereby unknowingly allowed a ransomware infection to compromise your computer, consider using resources like the Bleeping Computer Forums and ID Ransomware for professional troubleshooting assistance.