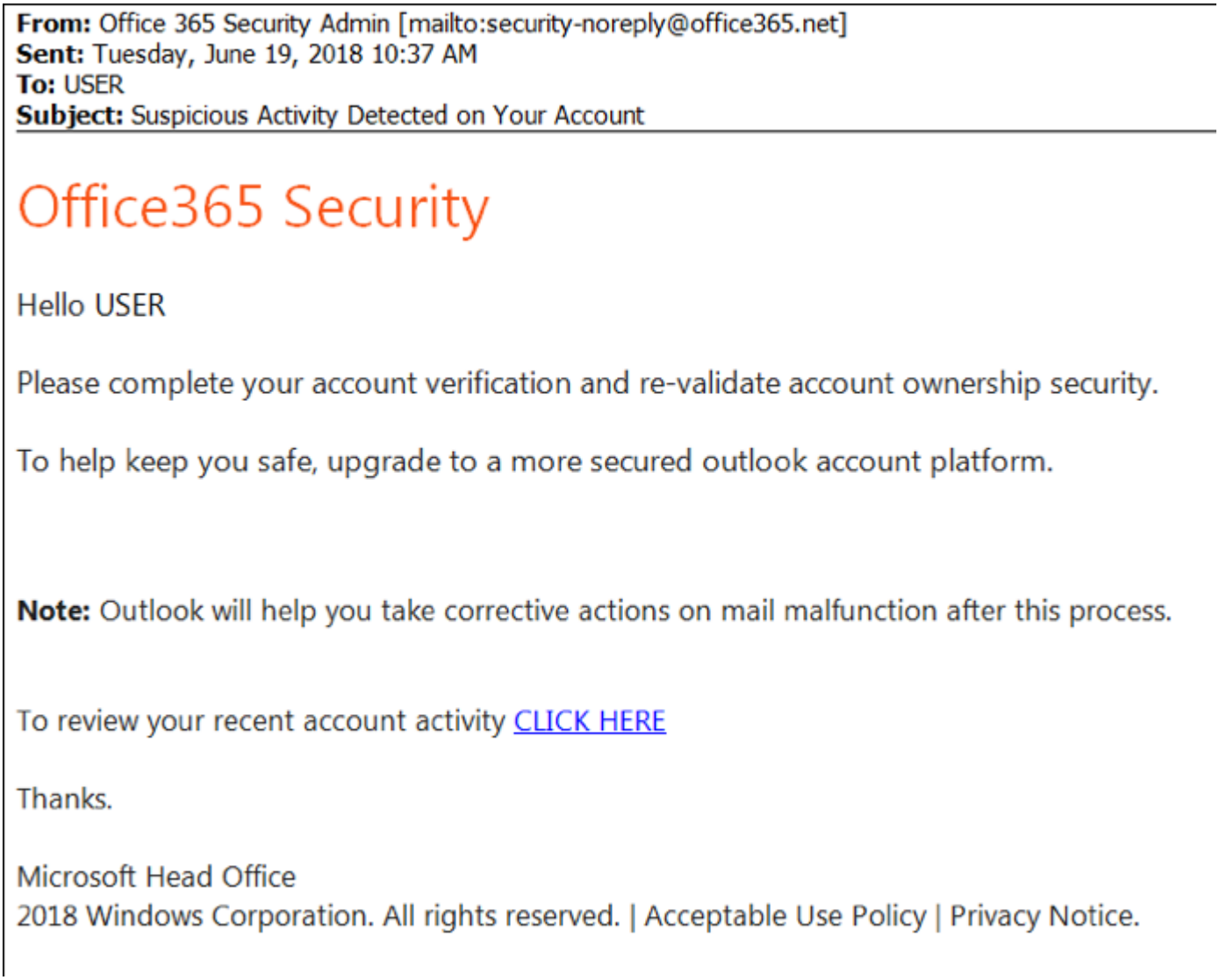
You receive an urgent phone call from a woman who claims to be an IRS agent. She says there's been an issue with your tax bill. She asks for your banking information to process the payment. It sounds serious.

It's easy to see why scams such as these are successful. Criminals convince people to act by assuming a position of authority and creating a sense of urgency. This type of cyber-attack is called social engineering. It leverages social tendencies to trick victims into taking a particular action.

When this scam takes place via email, it's called phishing. A single phishing campaign can bring in millions, making it lucrative for cybercriminals. In 2017 a phishing email sent to Google and Facebook employees resulted in $100 million wired to a cybercriminal overseas (**Fortune (https://fortune.com/2017/04/27/facebook-google-rimasauskas/)**). Thankfully, one of the best protections against phishing is in your hands. To defend against these attacks, you must learn how to spot suspicious emails.

Phishing attacks have come a long way since the famous "prince-who-will-wire-you-money" scam. Today they leverage spoofed email addresses. They'll include proper grammar and will use a malicious attachment or link to spur activity. Sometimes the link will lead to a site that appears legitimate, like an email or bank login page. But, it is actually spoofed and collecting user credentials maliciously. In other cases, the email will include an attachment which might be malware. Let's dive in with a few examples.

Example 1: Suspicious login attempt



From: Office 365 Security Admin [mailto:security-noreply@office365.net]
Sent: Tuesday, June 19, 2018 10:37 AM
To: USER
Subject: Suspicious Activity Detected on Your Account

Office365 Security

Hello USER

Please complete your account verification and re-validate account ownership security.

To help keep you safe, upgrade to a more secured outlook account platform.

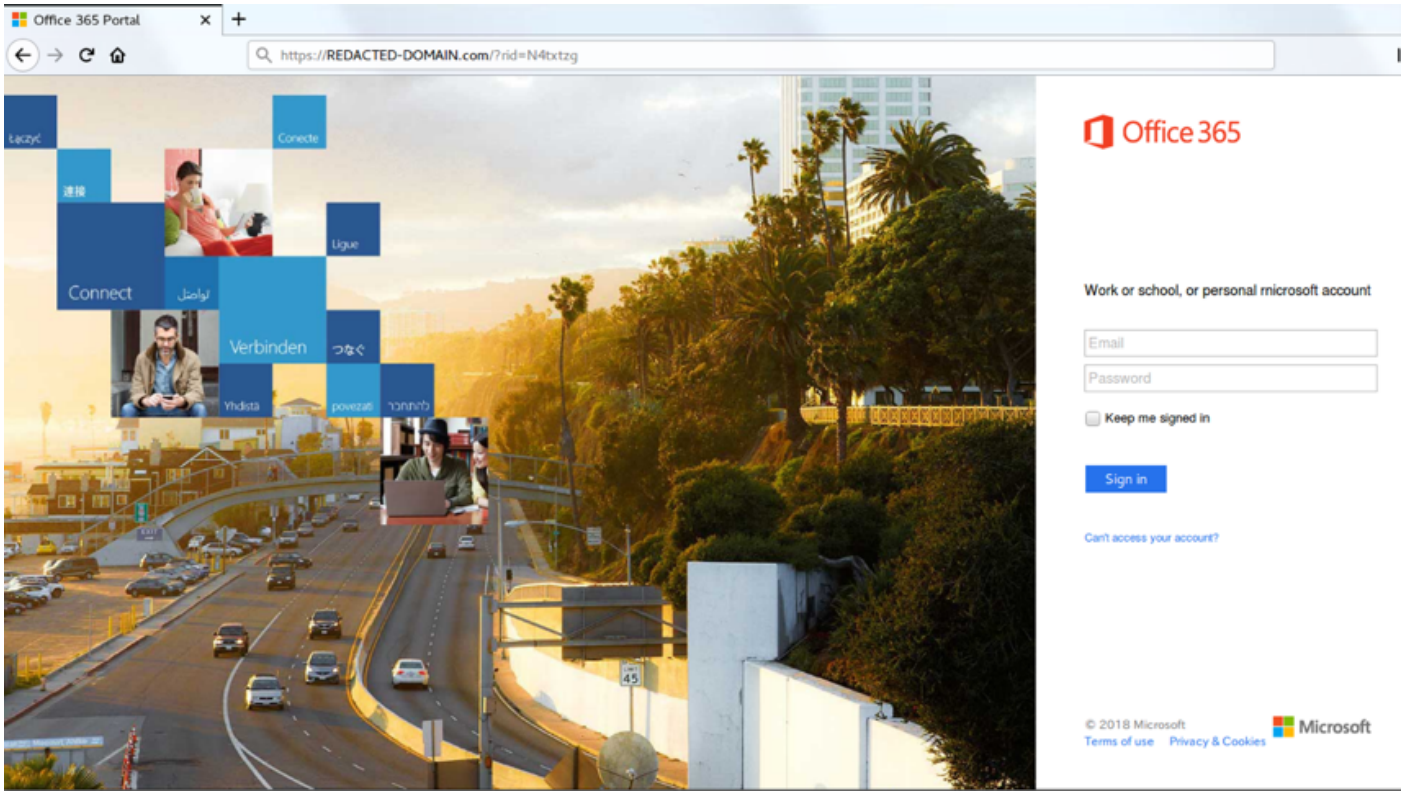
Note: Outlook will help you take corrective actions on mail malfunction after this process.

To review your recent account activity CLICK HERE

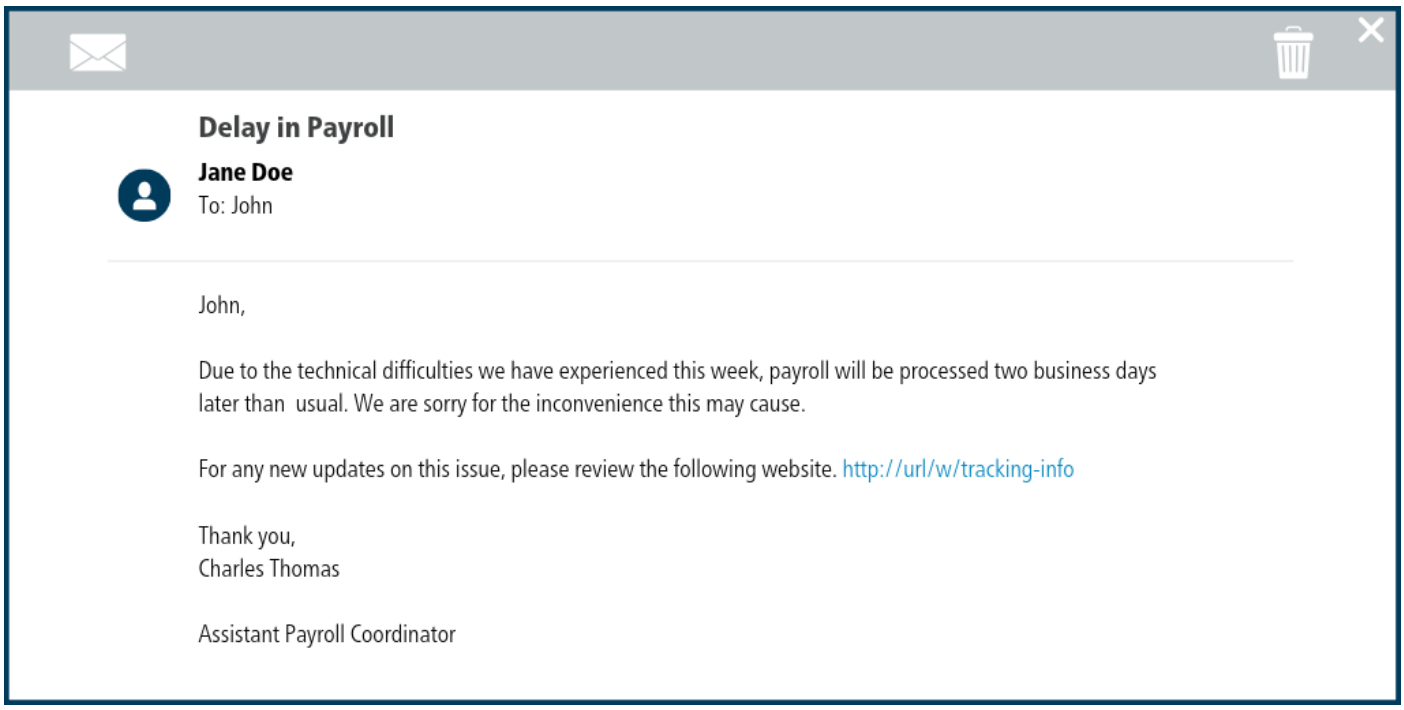
Thanks.

Microsoft Head Office
2018 Windows Corporation. All rights reserved. | Acceptable Use Policy | Privacy Notice.

After clicking on the link in this phishing email, the user is directed to a website that appears to be a legitimate login page. However, a close look will show that the domain is not from Microsoft.

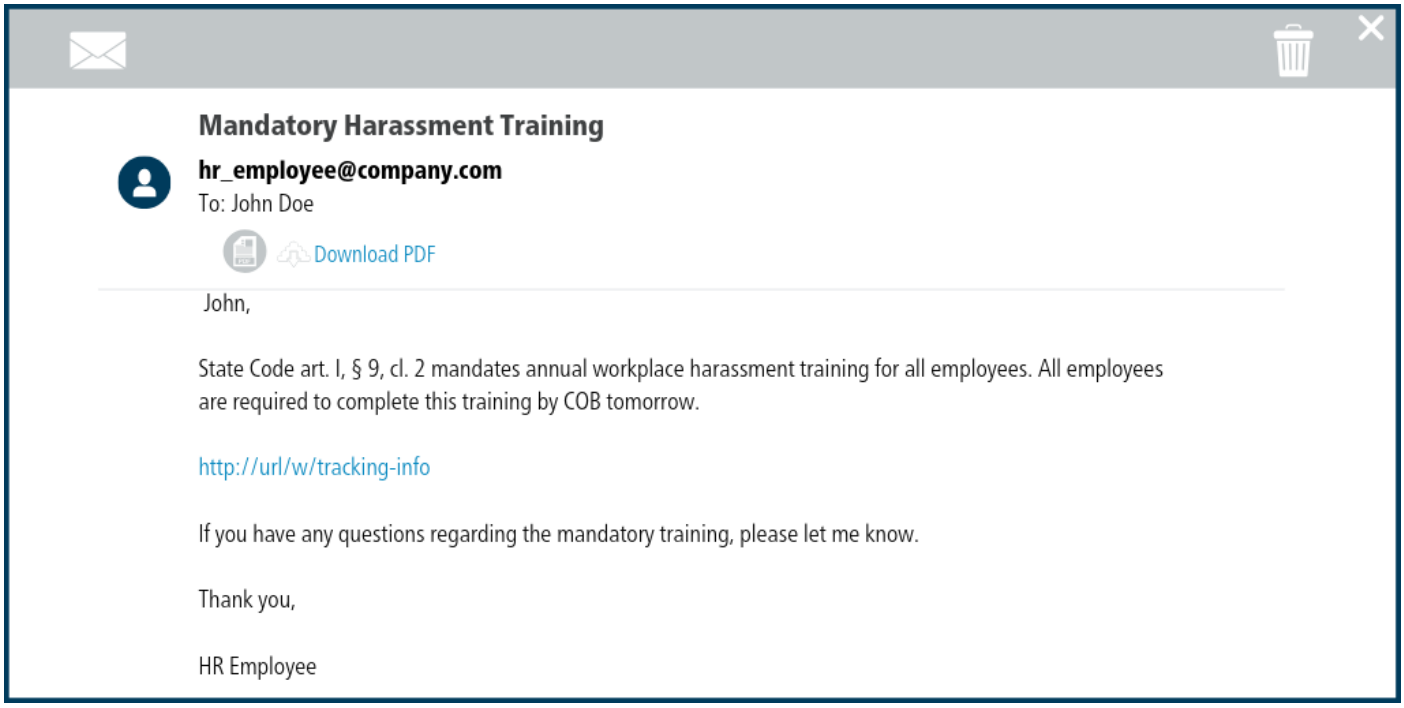


Example 2: Malicious link



In this example, the email content seems urgent – but the link is actually malicious. Cybercriminals leverage the recipient's innate desire to act in order to attract clicks.

Example 3: Malicious file



The attachment, in this case, could be malware made to look like a PDF. TIP: Never open or download email attachments that aren't from trusted senders.

Here's what to do if you spot a suspicious email: notify your IT security team or CISO (Chief Information Security Officer). They may have policies in place for handling suspected phishing. Examples include forwarding the email to a secure inbox for analysis or deleting it from your inbox. Above all, do not click on any links or download attachments if you do not know the email sender. Remember, legitimate organizations will never ask for sensitive information via an unsolicited email.

Teaching employees how to spot phishing emails is key to defending against attacks. Make sure they know what to do if they spot a suspicious email, such as:

- Don't open the email, click on any links, or download/open any attachments
- Report the email to your IT security team
- Follow organizational security policies

CIS offers phishing services to help organizations test their cyber defenses. Our cybersecurity experts work with IT teams to create a customized phishing email that emulates a real-world attack scenario. At the end, we develop a report to identify the methodology used and a breakdown of the results. The report also comes with a list of recommendations to assist with the mitigation and handling of a potential phishing attack.

LEARN ABOUT CIS PHISHING ENGAGEMENT SERVICES

ABOUT

PRODUCTS AND TOOLS

FOR SLTT GOVERNMENTS

EXPLORE

(https://twitter.com/CISecurity/)

(https://www.facebook.com/CenterforInternetSecurity)

(https://www.youtube.com/user/TheCISecurity)

(https://www.linkedin.com/company/center-for-internet-security)

orl
nt
Se
c/)

curi
ity/
)

pa
ny
/t
he
-
ce
nt
er-
for
-
int
er
ne
t-
se
cu
rit
y/
)