Outsmarting phishing scams: A playbook for employees

ESET

Digital Security
Progress. Protected.

Are you prepared to outsmart a phishing scam?

While technology plays a significant role in digital security, the human element remains a critical factor. A staggering [74% of breaches](#) in 2022 involved some kind of human error, stemming from either gullibility, panic, or lack of attention. These cyber threats, commonly known as social engineering attacks, exploit human vulnerabilities to lure victims into unwittingly opening the door for hackers to infiltrate their systems.

By unraveling the deceptive nature of social engineering techniques and understanding how they operate, we'll to equip you with the knowledge and tools necessary to confidently navigate encounters with these malicious schemes. Together, we will strengthen our collective defences against phishing attacks and forge a resilient front in the ongoing battle for digital security.

Where can you encounter phishing?

In your e-mail
PHISHING
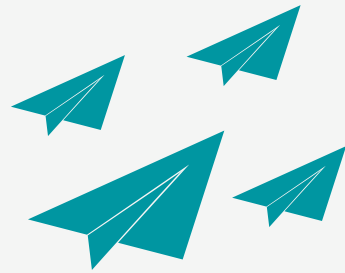
Phishing emails remain one of the most prolific cybercrime techniques, where attackers attempt to deceive you into revealing sensitive information, such as passwords, credit card details, or personal identification, by posing as a trustworthy entity. They typically work through malicious attachments or links that mimic legitimate websites.

In a text message
SMISHING

It is important to be aware that phishing messages can also be delivered by an SMS. The messages typically contain links that directs you to malicious websites, login pages, or apps. Once accessed, these channels may infect your device with malware and use it to extract your sensitive data.
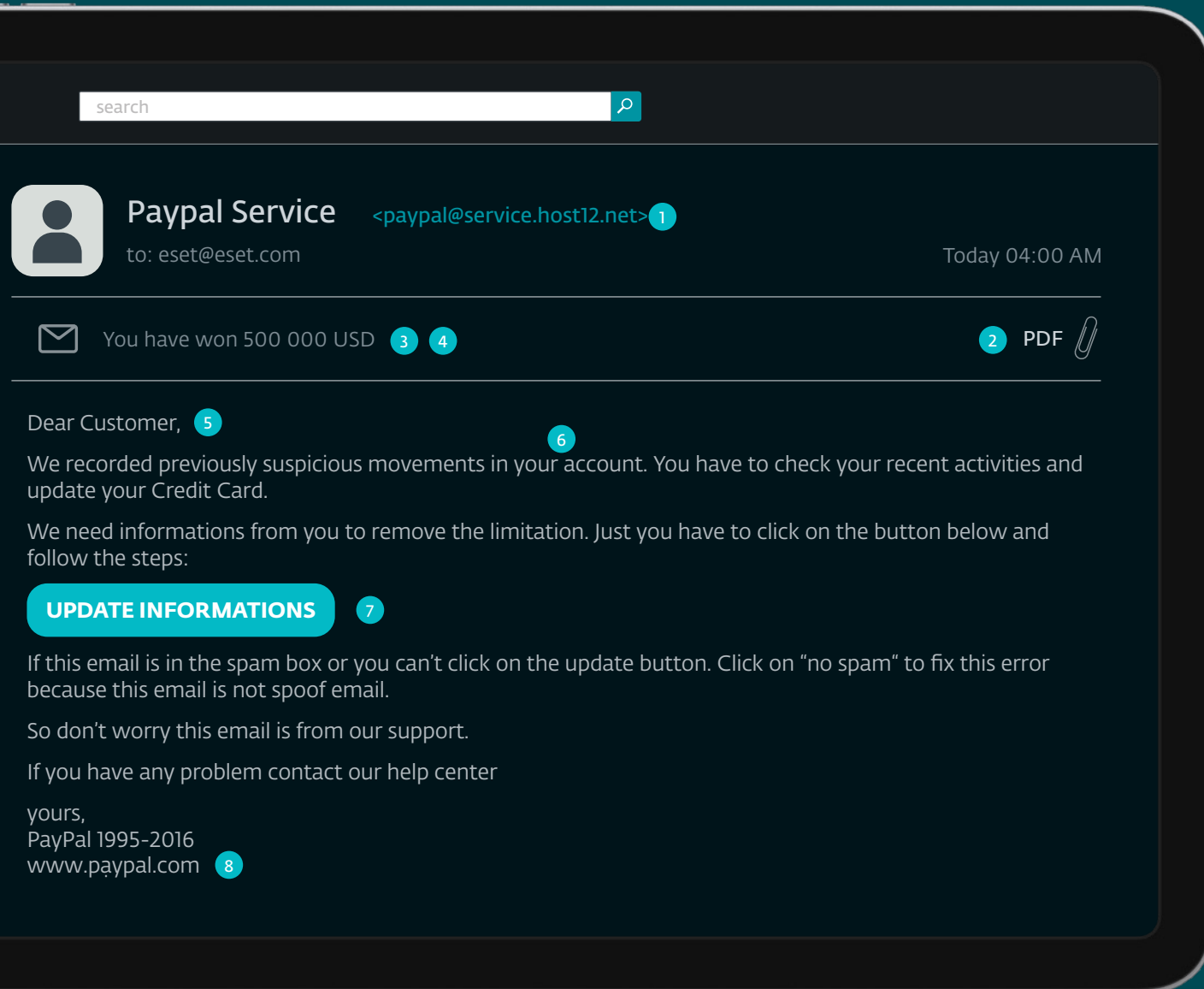
Over a phone call
VISHING

Scammers also use phone calls or voice messages to deceive you into divulging sensitive information or making fraudulent payments. The sophistication of these attacks ranges from human impersonators over automated robocalls to deepfakes of a person you know. Some scammers even employ call spoofing, using legitimate phone numbers to enhance this deception.

How to recognise a phishing e-mail?
Look for these characteristics:

Paypal Service <paypal@service.host12.net> **1**
to: eset@eset.com

Today 04:00 AM

✉ You have won 500 000 USD **3** **4**

2 PDF 📎

Dear Customer, **5**

We recorded previously suspicious movements in your account. You have to check your recent activities and update your Credit Card. **6**

We need informations from you to remove the limitation. Just you have to click on the button below and follow the steps:

UPDATE INFORMATIONS **7**

If this email is in the spam box or you can't click on the update button. Click on "no spam" to fix this error because this email is not spoof email.

So don't worry this email is from our support.

If you have any problem contact our help center

yours,
PayPal 1995-2016
www.paypal.com **8**

1 If you are not familiar with the email address, handle the contents with caution.

2 Expect the worst from attached files or unfamiliar links. They might contain malware or send you to a malicious web destination.

3 Too scary or too good to be true? It's probably a scam. Remember that social engineering specifically exploits human weaknesses.

4 The subject differs from the message.

5 If the greeting is too general it might be a sign that it was not addressed only to you, but a number of other people too.

6 Sense of urgency? The scammer wants you to panic.

7 Bad spelling and other grammatical errors are common in phishing mails that have been translated from other languages.

8 Homoglyph attacks rely on replacing characters in addresses with ones that look similar, but belong to different alphabets (like "a̦" vs. "a" in paypal.com).

Common phishing schemes

DEMANDS FOR PAYMENT

From: XERO Tuesday, 20 June 2017, 12:09 p.m.
To:

Subject: Your xero invoice available now.

Hi,
Thanks for working with us. Your bill for $373.75 was due on 28 Aug 2023.

If you've already paid it, please ignore this email and sorry for bothering you. If you've not paid it, please do so as soon as possible.

To view your bill visit https://in.xero.com/5LQDhR

If you've got any questions, or want to arrange alternative payment don't hesitate to get in touch.

Thanks
NJW Limited

Download PDF

Scammers pose, for example, as government agency representatives, threatening with fines or arrests if payment is not made. Other examples include the attacker posing as the company's CEO, asking for quick payment from one of the employees, or suppliers contacting employees, demanding compensation for packages and goods.

ACCOUNT VERIFICATION

New Message

To: David
From: GlobalPay <VT@globalpay.com>

Subject: Restore your account

Date: February 7, 2014 3:47:02 AM MST

Dear customer,

We regret to inform you that your account has been restricted.

To continue using our services please download the file attached to this e-mail and update your login information.

© Global Payments Inc

update2816. html (7kb)

Scammers often impersonate, among other financial institutions, entertainment platforms such as Netflix, or digital stores, where users have personal profiles. They may claim unusual activity on the account, lead users to fake websites, and request login information for verification purposes.

PROGRAM ENROLLMENT

CENTRAL MEDICAL

Open Enrollment Period Has Arrived!

Welcome
Open enrollment is now open for all existing and new employees. To use our online system to streamline your enrollment and take advantage of your health insurance please create and/or sign in.

Company: Hook Security Team
Policy ID: 8402 428 4992 1
Status: Open Enrollment

Thank you,
Central Medical Team

REGISTER   **SIGN IN**

Scammers pretend to be government program representatives, offering assistance with enrollment while collecting personal and financial data. This can include fake emails with invitations to webinars and other events, where users create accounts with a password. This is a problem primarily if the person uses the same password for different accounts because it gives the scammer a free pass to hijack them.

Common phishing schemes

ORDER/SHIPPING CONFIRMATION

We are happy to inform you that our online store HomeDepot.com has an order whose recipients details match yours. The order could be received in any Local Store of HomeDepot.com within the period of 5 days.

Open this link to see full information about your order.

Our blessings to you on a Thanksgiving Day! HomeDepot.com

Victims receive fake links to track nonexistent packages or confirm orders, leading to the extraction of login credentials or malware installation. This can later be used to infiltrate other websites with the same logins. It is essential not to click suspicious links, and to check any incoming emails for the telling signs of a scam.

WINNING A PRIZE

JBSStore

Text Message

Dear Leigh! This morning JB Store announced their lottery winners. Congratulations you took 2nd place. Check what you won http://rtapit.com/7FA

Today 12:45pm

Scammers inform individuals of a contest victory, and then request personal information or access to their bank accounts. Personal data can then be extracted from the accounts, potentially causing significant financial damage. It is essential to verify any contest victories through the official organiser.

TECH SUPPORT

Hello, this is Micheal from IT department. I was tasked with installing new updates on your computer. I tried to do it remotely but there seems to be some technical issue. If we don't do this now it may result in your mailbox failing to connect to the company server, so you wouldn't be able to receive or send any emails. Can you tell me your password so I can try to solve it immediately?

Scammers pose as IT support and ask users to provide their access login credentials, claiming they need to fix or update something on their computers remotely. This allows scammers to gain access to personal data and sensitive information. It is important to remember that IT or HR departments usually don't ask employees to share private information over the phone, or through email.

How to react if you receive a suspicious message or a call?

1
PAUSE, THINK, AND ACT

Scammers rely on the urgency to manipulate victims. Take time to evaluate requests and prevent hasty action. Avoid clicking on links in messages, and visit the organisation's official website to verify the communication's legitimacy.

2
BE SUSPICIOUS OF UNKNOWN NUMBERS

Verify calls or text messages from unfamiliar or suspicious numbers. Avoid disclosing any personal information or clicking unknown links within messages. This helps you minimise the chances of falling victim to such scams.

3
DON'T INTERACT WITH THE SCAMMERS

Scammers use emotional manipulation to exploit their victims, so interacting with them increases your risk of falling for their schemes. In some cases, scammers may become more aggressive or persistent if they sense that you are willing to engage with them. They will also use any information you give them against you. Overall, talking to scammers is draining, dangerous and completely ineffective.

4
VERIFY IDENTITY

If you receive a message from someone claiming to represent a company or government agency, avoid interacting directly. Instead, independently verify their authenticity by contacting the organisation using the official contact information available on their website.

5
ENABLE STRONG SECURITY MEASURES

Use strong and unique passwords to protect your accounts. Consider utilising password generators and managers to create long and complex passwords or passphrases, and store them securely. Use Multi-Factor Authentication (MFA) whenever available to add an extra layer of protection.

Still not sure if the message you received is dangerous? Here's what you can do:

If the suspicious email contains a link to a webpage:
Hover over the link to see the URL. If the address does not correspond to the content or the sender of the email, do not click on it. If you have even the slightest doubt, do not click on any links. Remember, the phishing message cannot harm you unless you click on a link or open an attachment.

If the sender's address seems familiar to you, but the content of the message doesn't make sense to you:
You can contact the sender via a new email to verify the authenticity of the email.

If it looks like a message from a cloud service:
Various cloud services are often abused. By hosting phishing websites on legitimate servers, like Microsoft Azure or OneDrive, phishers are able to present legitimate domains. Read such an email several times.

Any web address where you plan to enter personal information should be preceded by "https:"
The letter "s" means "secure." If you don't see "https," you're not in a secure web session, and you shouldn't enter any personal information. However, if you see "https," it is still not a guarantee that you are not being phished.

Phishing messages can be obvious scams or be quite sophisticatedly disguised. If you are not sure if the message is legitimate (or you are sure it is not), **it is always a good idea to report it to your company's IT Security or other appropriate authorities.**

With the insights and practical tips included within this playbook, you will be well-prepared to navigate the treacherous waters of phishing attempts with caution and confidence. As you embrace these strategies and integrate them into your digital practices, you will become an active participant in fortifying your organisation's collective resilience against cyber threats.

Digital Security
Guide

The Digital Security Guide is curated and supervised by cybersecurity experts at ESET who share their know-how and experience to help small and medium-sized businesses build an effective cybersecurity infrastructure. Protecting your business by implementing high-quality digital security solutions means protecting your progress. For more than 30 years, ESET® has been developing industry-leading IT security software and services to protect businesses, critical infrastructure, and consumers worldwide from increasingly sophisticated digital threats. For more information, visit www.digitalsecurityguide.eset.com or follow ESET on LinkedIn, Facebook, and Twitter.