85% of security breaches involve a human element

Phishing is one of the most effective and widespread techniques used by cyber criminals to gain access to a company's system and information.

The best way to mitigate this risk is to strengthen our human firewall.

You can help by learning how to recognize and report phishing attacks.

This will help to protect yourself, your colleagues, and your organization!

The impact of a security breach

What can happen when the cybercriminals are successful?

Money lost

A breach caused by phishing costs businesses an average of $4.65 million per breach.

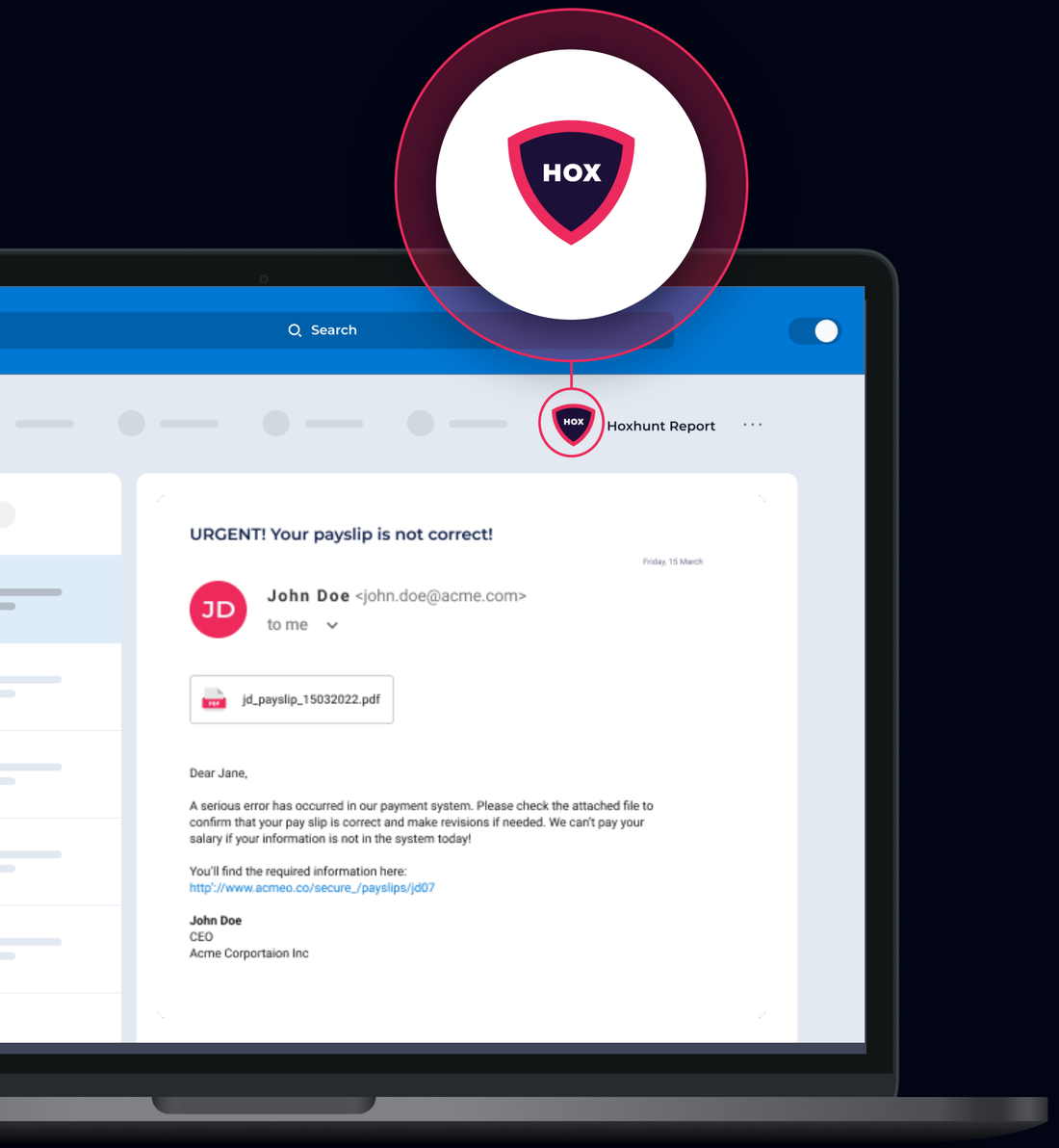
Business interrupted

Business operations will often be heavily disrupted in the aftermath of a security breach.

Data abused

Passwords and personally identifiable data can then be used in a wide variety of fraud, impersonation schemes, and scams. The breached information can circulate on the dark web for 200+ days.

Want to learn more?
Why should you report suspicious emails and how do you do it?



How to detect a suspicious email

Always report an email if you find some of the following elements suspicious:

1. Sender: Do you know the sender or are they relevant to your company or to yourself? Click on the sender's name to see the email address.

2. Attachments: Are you expecting the attached file? Always consider if the attachment is relevant to you.

3. Actions: Is there a sense of urgency? Consider the authenticity of an email before taking any actions.

4. Links: Hover your mouse over the links to see the original URL. You can also copy the link URL with right-click and paste it somewhere you can read it.

Every push of the button makes you smarter, stronger, and safer

When you see a suspicious email, report it with the Hoxhunt button. You can help stop an attack in its tracks!

WANT TO LEARN MORE?

Why should you report suspicious emails and how do you do it?