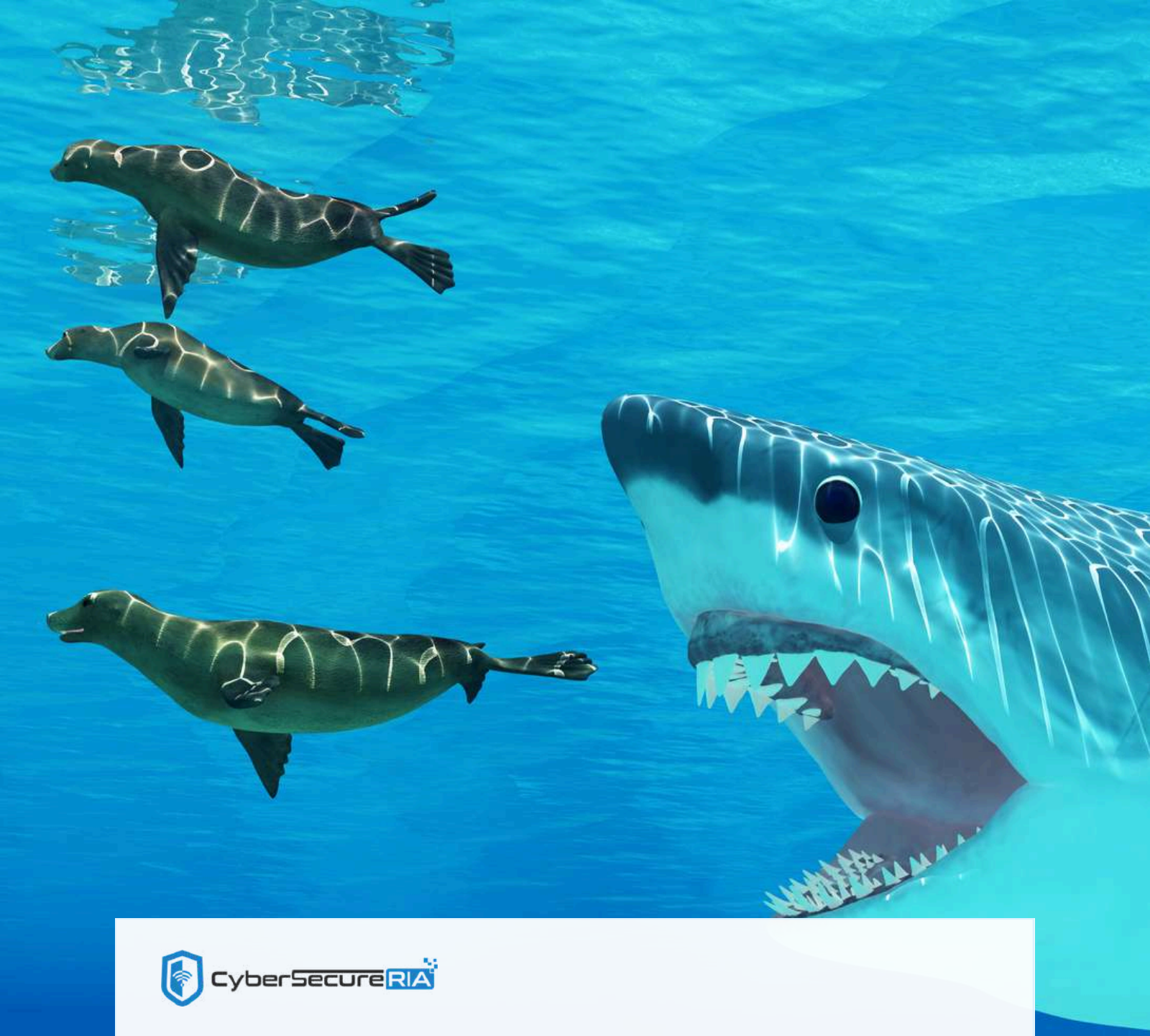
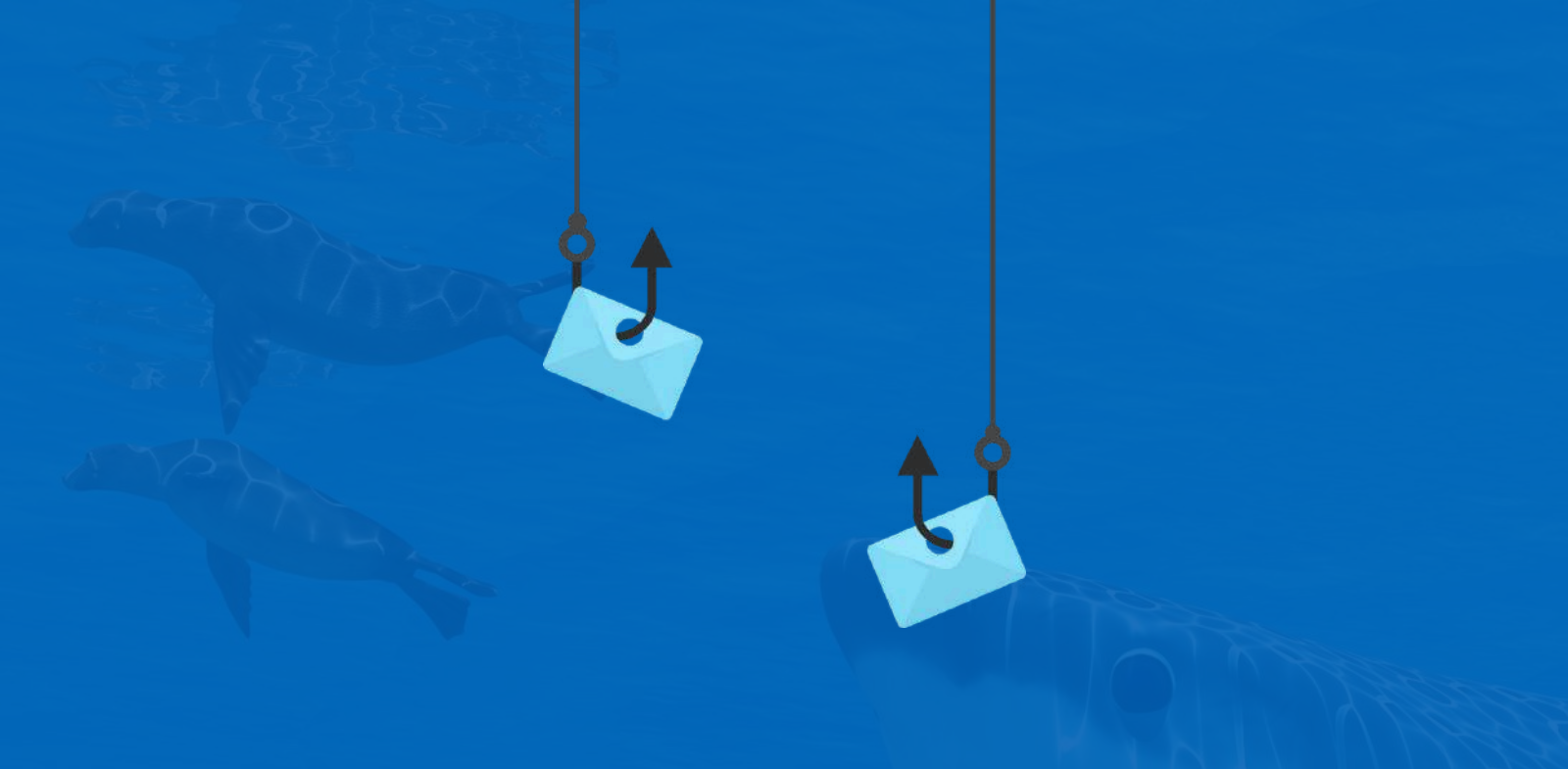


CyberSecureRIA

SOCIAL ENGINEERING ATTACKS

AFTER YOUR EMPLOYEES



Cybercriminals are after your employees, not because they're careless but because they're human. Hackers use social engineering attacks to trick their victims, as it saves them from the difficult work of getting around a firewall or antivirus. Let's dive into some of the deceptive tactics they use to exploit your employees.

ATTACK #1

PHISHING

Hackers target the very thing that an employee checks every day— their email inbox.

Phishing emails pose as someone trustworthy, like a manager, a vendor or IT. Their ulterior motive is to trick your employees into clicking on compromised links, downloading files or giving away login details.

To	youremail@gmail.com
From	security@support-notice.com
Subject	URGENT - UPDATE ACCOUNT!

Dear User,

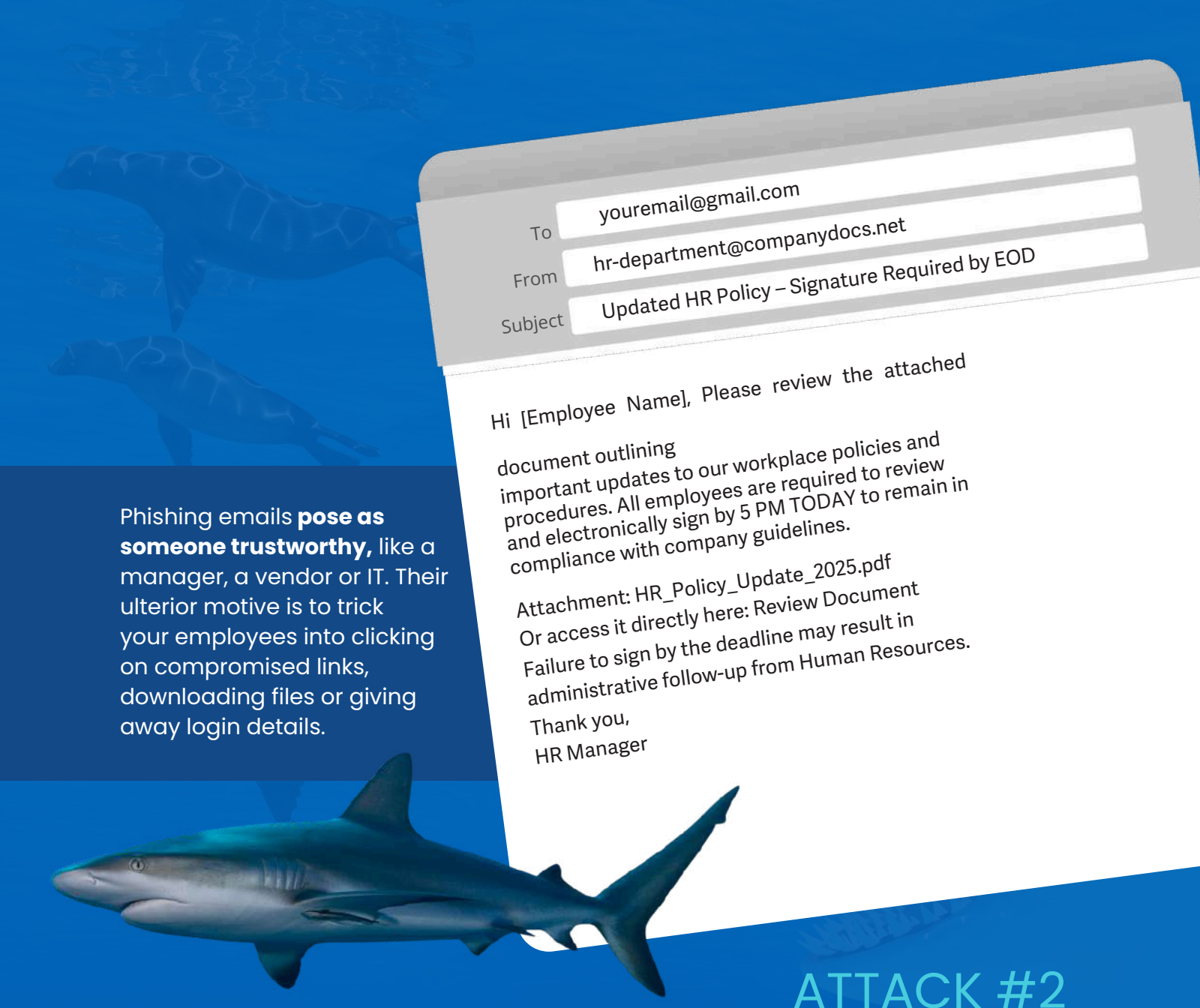
We have detected unusual activity on your account and, as a precaution, have temporarily restricted access. To avoid **PERMANENT SUSPENSION,** you must verify your identity and reset your password immediately!!

Please follow the link below to restore acces:

Reset Your Password Now

This link will expire in 2 hours. Failure to act will result in the deactivation of your account for security reasons.

Thank you for your prompt attention to this matter.
Sincerely, Account Security Team



Phishing emails **pose as someone trustworthy,** like a manager, a vendor or IT. Their ulterior motive is to trick your employees into clicking on compromised links, downloading files or giving away login details.

ATTACK #2

SPEAR PHISHING

This is a highly personalized social engineering attack in which the hacker uses personal or work-related information to mislead your employees.

ATTACK #3

PRETEXTING

Unlike phishing attacks, where the perpetrators induce panic or urgency, in pretexting, scammers take time to build trust by using carefully crafted stories.

The hacker could pose as an IT technician or HR and **create a believable story to gain your trust.** They can claim that there has been a breach and they can help, but only if you share your credentials or grant access to your laptop. It sounds like an offer to help but it's a trap.

ATTACK #4

QUID PRO QUO (QPQ):

In this phishing scam, the attacker uses their social skills to convince the victim that they're doing them a favor and for free.

They could even pose as a trusted source like a penetration testing company but, in turn, may ask you to share sensitive information or manipulate you to install malware into your systems.

ATTACK #5

BAITING

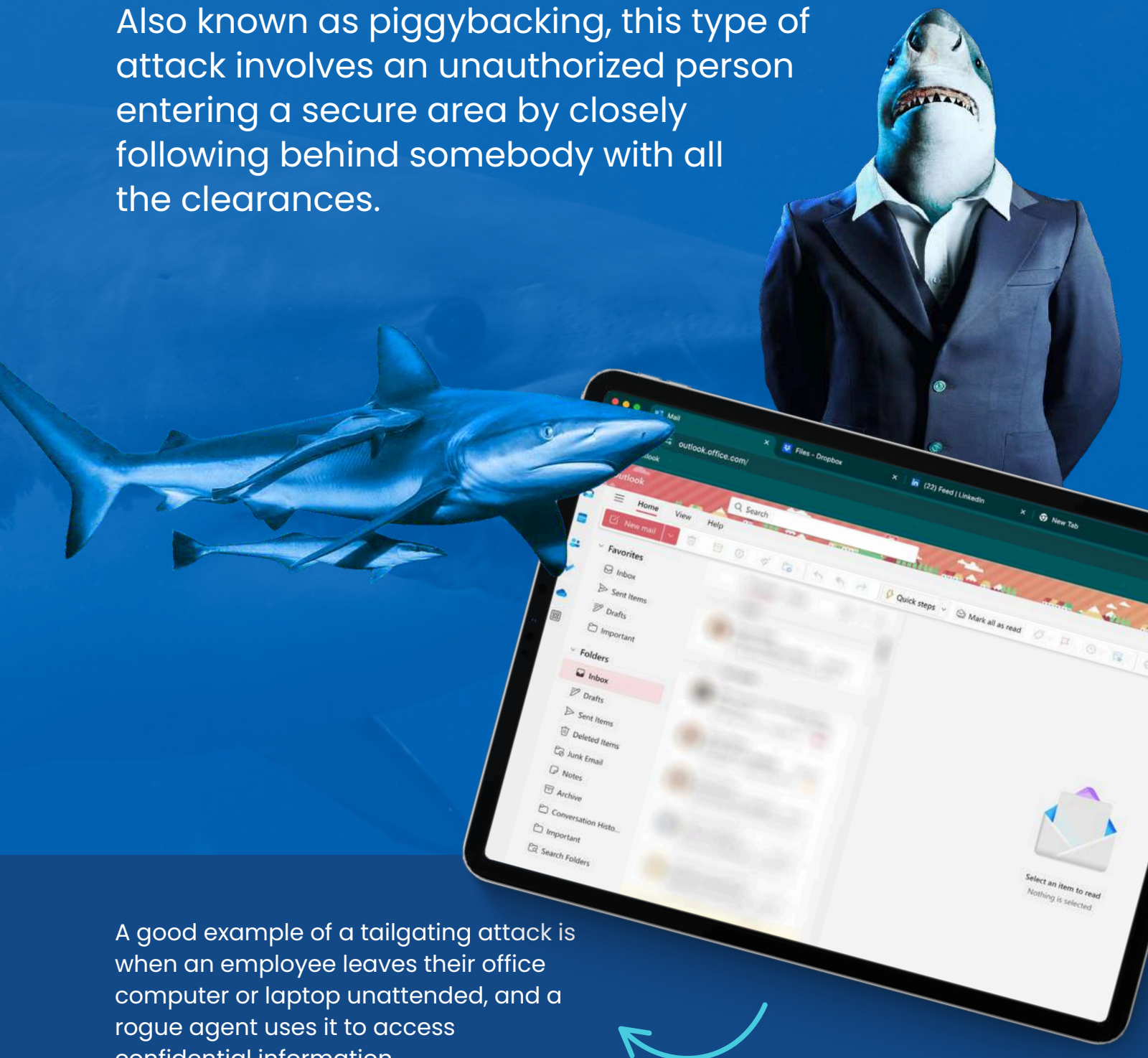
The most famous, or rather infamous, example of this social engineering attack is the Nigerian Prince scam.

They could even pose as a trusted source like a penetration testing company but, in turn, may ask you to share sensitive information or manipulate you to install malware into your systems.

ATTACK #6

TAILGATING

Also known as piggybacking, this type of attack involves an unauthorized person entering a secure area by closely following behind somebody with all the clearances.



A good example of a tailgating attack is when an employee leaves their office computer or laptop unattended, and a rogue agent uses it to access confidential information.

The hacker looks for vulnerabilities and exploits the watering hole website to carry out a full-scale attack on the targeted business. Often, infected malware is used in such attacks.

ATTACK #7

WATERING HOLE

This is a highly sophisticated attack in which the hacker identifies a frequently visited website within the targeted business.

CyberSecureRIA

TURN YOUR EMPLOYEES INTO YOUR STRONGEST DEFENSE.

CONTACT US TO **FORTIFY YOUR BUSINESS!**