7 SOCIAL ENGINEERING ATTACKS **AFTER YOUR EMPLOYEES**

Call Cicom 1300 324 266

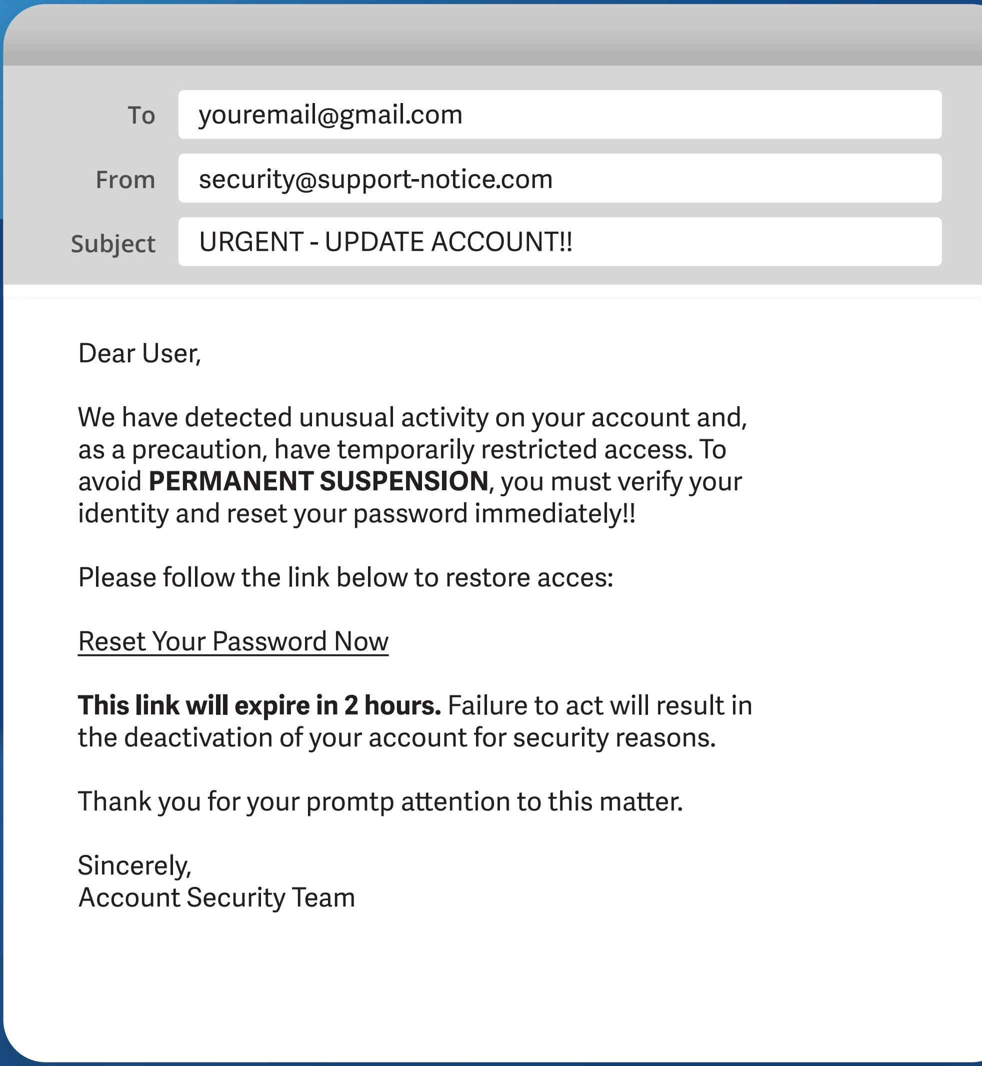
Cybercriminals are after your employees, not because they’re careless but because they’re human. **Hackers use social engineering attacks to trick their victims,** as it saves them from the difficult work of getting around a firewall or antivirus. Let’s dive into some of the **deceptive tactics they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

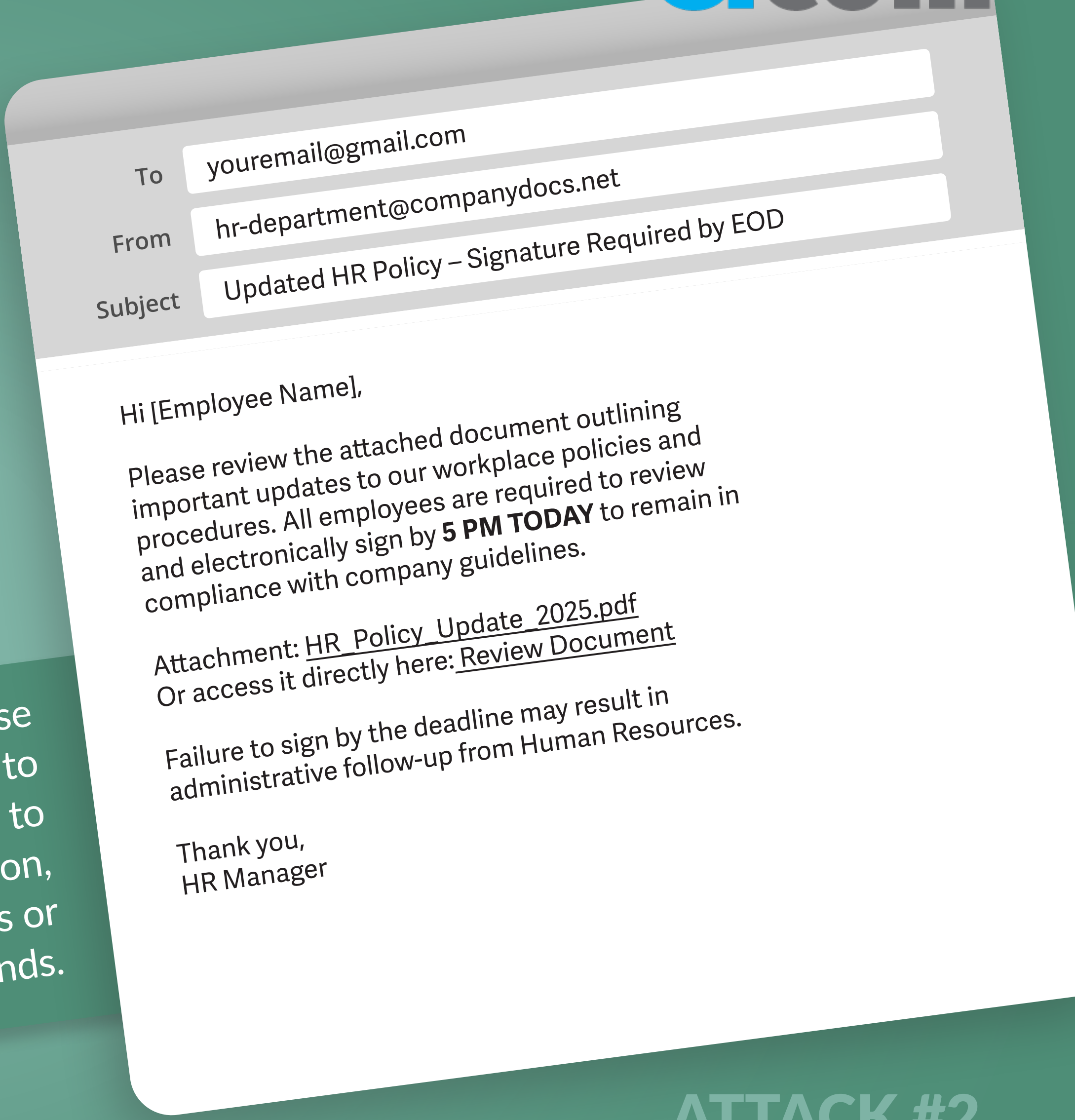
Reset Your Password Now

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 promptp attention to this matter.

Sincerely,
Account Security Team

Call Cicom 1300 324 266



To youremail@gmail.com

From hr-department@companydocs.net

Subject Updated HR Policy – Signature Required by EOD

Hi [Employee Name],

Please review the attached document outlining important updates to our workplace policies and procedures. All employees are required to review and electronically sign by **5 PM TODAY** to remain in compliance with company guidelines.

Attachment: HR_Policy_Update_2025.pdf
Or access it directly here: Review Document

Failure to sign by the deadline may result in administrative follow-up from Human Resources.

Thank you,
HR Manager

Their goal is to use **familiarity as bait** to convince an employee to share sensitive information, download malicious files or transfer funds.

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.

Call Cicom 1300 324 266

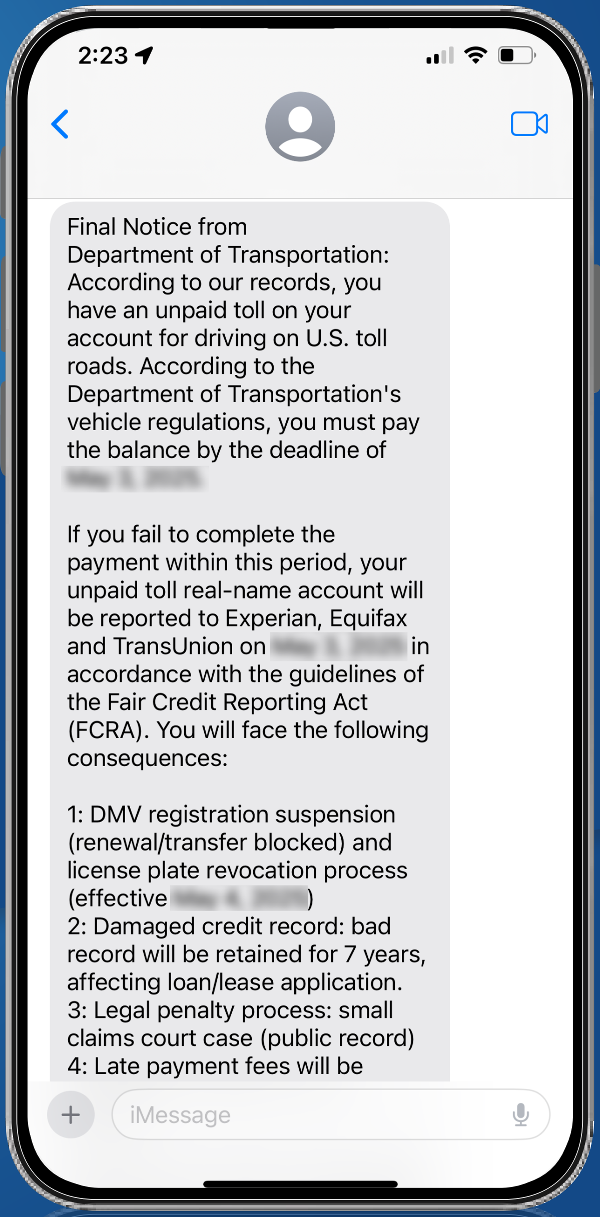
Cicom®

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.



Final Notice from Department of Transportation: According to our records, you have an unpaid toll on your account for driving on U.S. toll roads. According to the Department of Transportation's vehicle regulations, you must pay the balance by the deadline of [redacted]

If you fail to complete the payment within this period, your unpaid toll real-name account will be reported to Experian, Equifax and TransUnion on [redacted] in accordance with the guidelines of the Fair Credit Reporting Act (FCRA). You will face the following consequences:

1: DMV registration suspension (renewal/transfer blocked) and license plate revocation process (effective [redacted])
2: Damaged credit record: bad record will be retained for 7 years, affecting loan/lease application.
3: Legal penalty process: small claims court case (public record)
4: Late payment fees will be

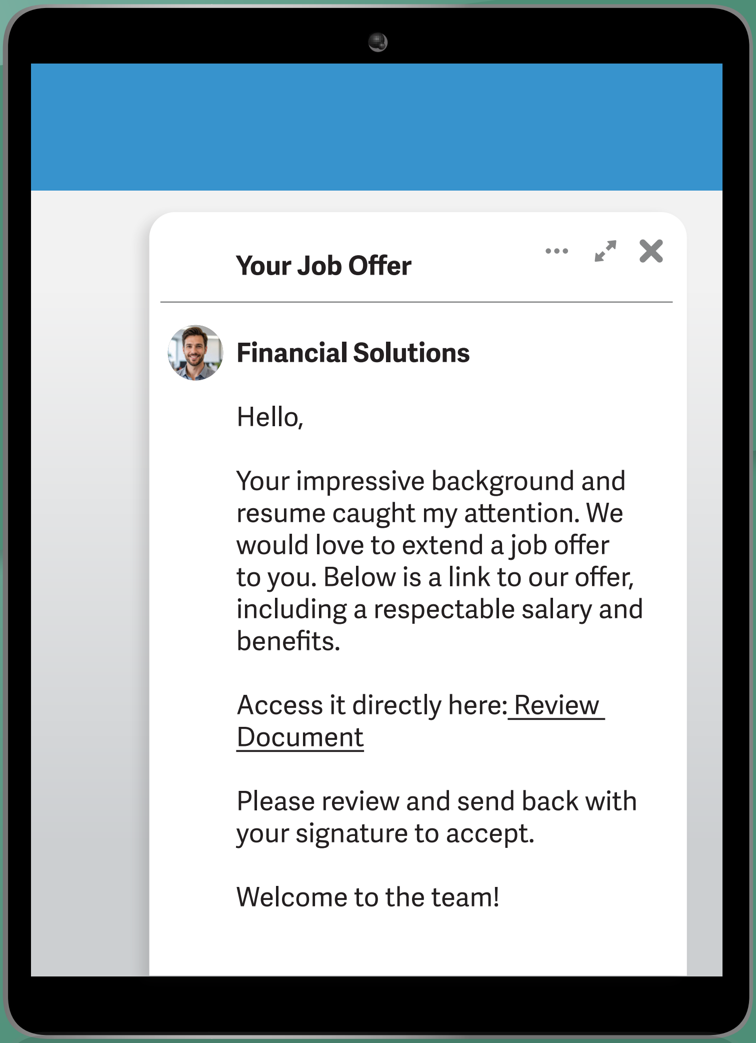
Call Cicom 1300 324 266

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.



Your Job Offer

Financial Solutions

Hello,

Your impressive background and resume caught my attention. We would love to extend a job offer to you. Below is a link to our offer, including a respectable salary and benefits.

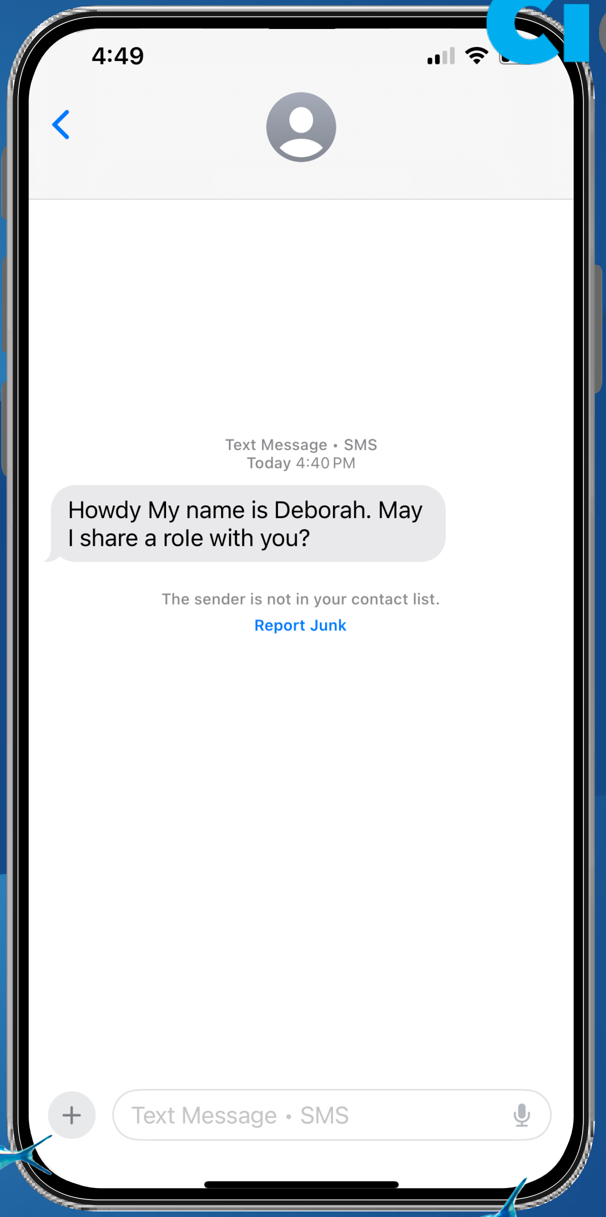
Access it directly here: Review Document

Please review and send back with your signature to accept.

Welcome to the team!

Call Cicom 1300 324 266

The aim is to **entrap unsuspecting victims with a valuable offer** and, in return, the victims knowingly or unknowingly share sensitive information, transfer funds or end up downloading malicious malware.



Text Message • SMS
Today 4:40 PM

Howdy My name is Deborah. May I share a role with you?

The sender is not in your contact list.
Report Junk

ATTACK #5

BAITING

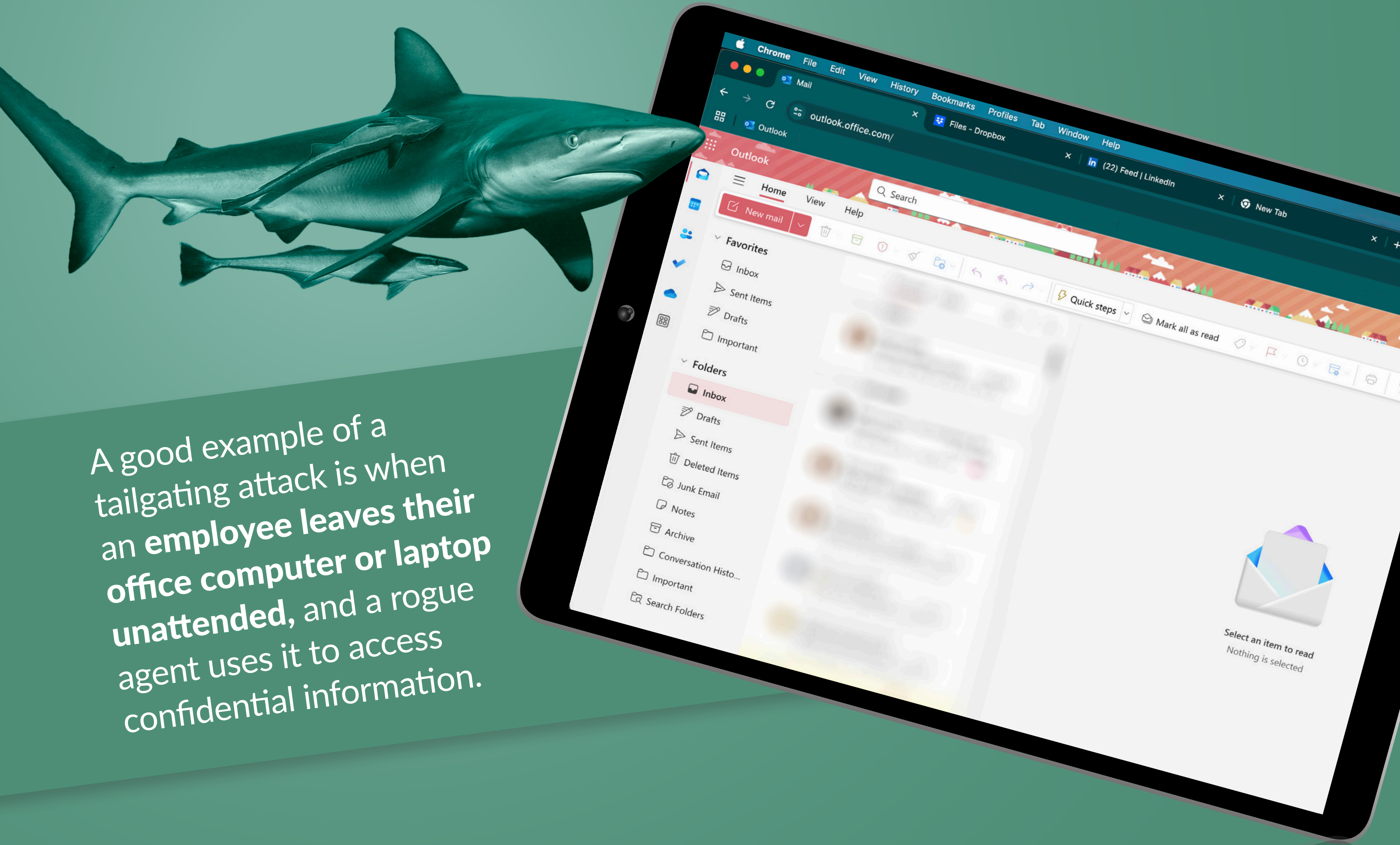
The most famous, or rather infamous, example of this social engineering attack is the Nigerian Prince scam.

Call Cicom 1300 324 266

ATTACK #6

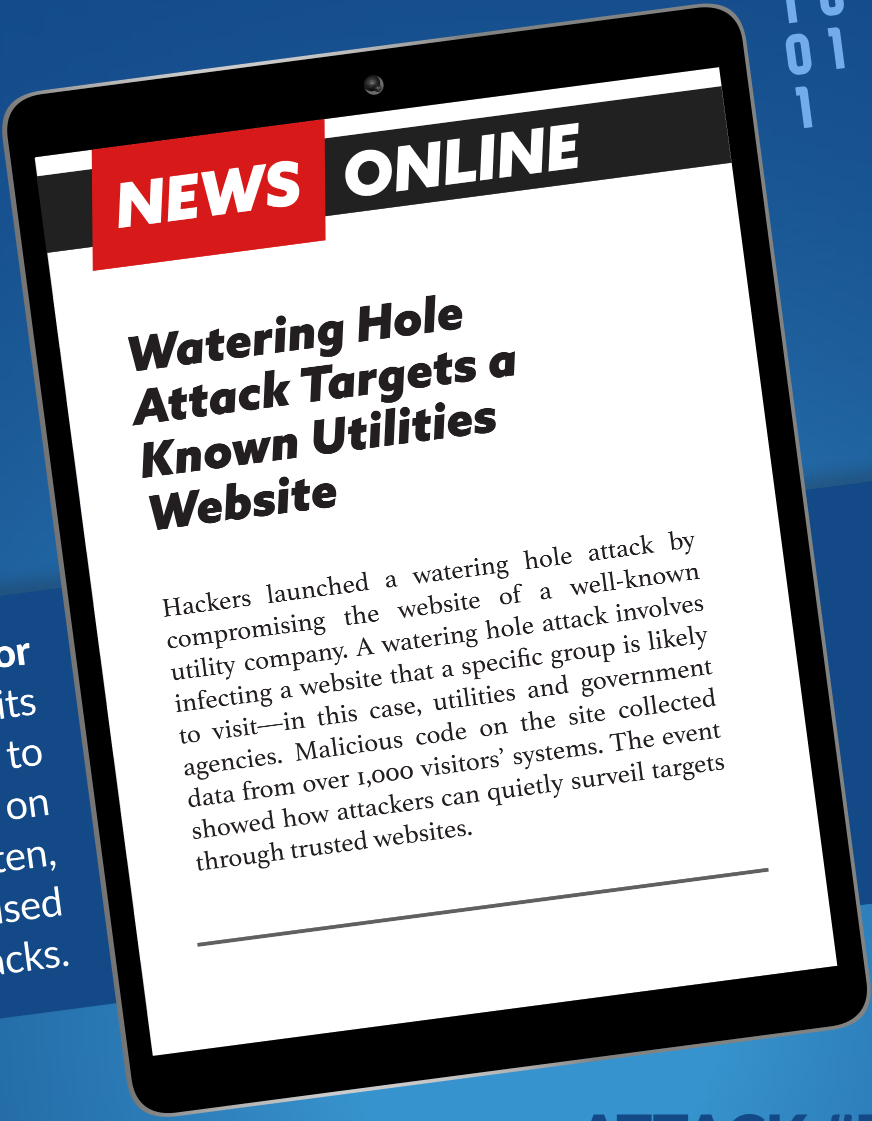
TAILGATING

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.

Call Cicom 1300 324 266



NEWS ONLINE

Watering Hole Attack Targets a Known Utilities Website

Hackers launched a watering hole attack by compromising the website of a well-known utility company. A watering hole attack involves infecting a website that a specific group is likely to visit—in this case, utilities and government agencies. Malicious code on the site collected data from over 1,000 visitors' systems. The event showed how attackers can quietly surveil targets through trusted websites.

The hacker **looks for vulnerabilities** and exploits the watering hole website to **carry out a full-scale attack** on the targeted business. Often, 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.

Call Cicom 1300 324 266

Cicom®

TURN YOUR EMPLOYEES INTO YOUR STRONGEST DEFENSE.

CONTACT US TO **FORTIFY YOUR BUSINESS!**

Call Cicom 1300 324 266