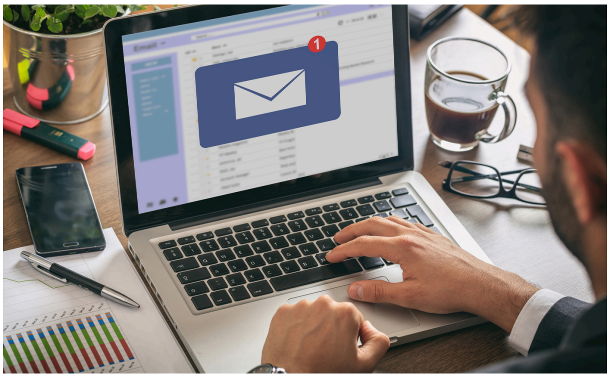
27 MARCH 2025

McLaren Strategic Solutions

Newsletter

PHISHING 101

Got Phished?



A phishing test was conducted using an email campaign impersonating the Microsoft Support Team from microsoft.mclarens.co.in. The email claimed the recipient's Outlook storage was full, urging them to click "Manage Your Mailbox" to free up space. This button led to a fake Microsoft login page designed to capture credentials. After submission, users were redirected to an error page, completing the test.

Let’s see how many of you took the bait!

⚠️ 19% clicked on the phishing link.

🚨 11% got phished!

The phishing assessment concluded that while some employees were susceptible to deceptive phishing attempts, a significant number exercised caution by refraining from engagement—a positive sign. However, there is room for improvement.
Starting with this newsletter, we are taking a step towards strengthening phishing awareness. Education is key—learning to identify phishing emails and avoiding malicious links is essential in defending against cyber threats. Strengthening training programs and reinforcing reporting procedures will further enhance our organization's security posture.

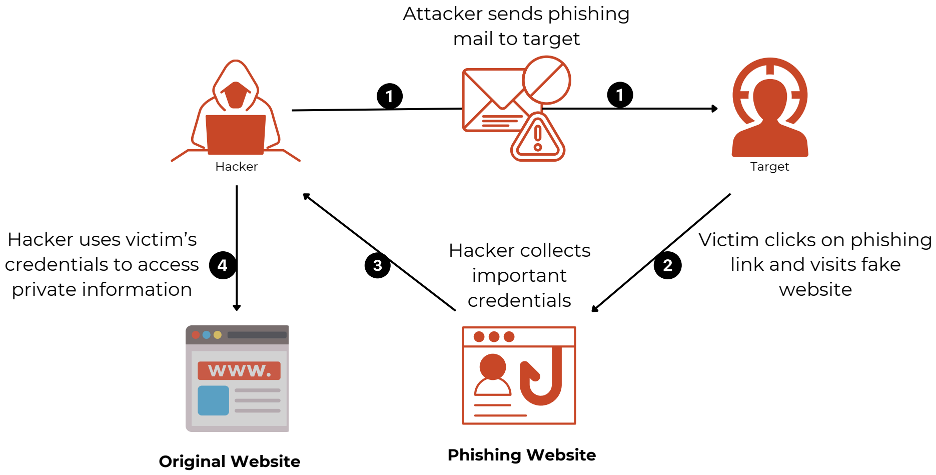
Phishing - An Overview

Phishing is a common cyber attack where attackers pose as trusted sources—via email, text, or calls—to trick people into sharing sensitive data like passwords or bank info.

It's a form of social engineering that uses deception and urgency. From fake links to malware, tactics have evolved. Since the 1990s, phishing has grown into types like spear phishing, smishing, vishing, and whaling—each with its own sneaky approach.

How Phishing Works?

The attacker tricks people by faking the sender's email to look like it's from a trusted source. The email reaches the inbox and seems real. It usually has a link that takes the user to a fake website that looks genuine. The user is then asked to enter login details or financial info, which goes directly to the attacker and is used for fraud or identity theft.


Attacker sends phishing mail to target
1
1
Hacker
Target
Hacker uses victim's credentials to access private information
4
3
Hacker collects important credentials
2
Victim clicks on phishing link and visits fake website
WWW.
Original Website
Phishing Website

🔍 How to Spot a Phishing Email

Phishing attacks are getting sneakier, but there are still some clear warning signs you can watch for. Here are some telltale signs that an email might be a phishing attempt:

- ❗ Urgent or Threatening Language
- 👋 Unfamiliar or Generic Greetings
- 📎 Unexpected Attachments or Files
- 🕵️ Too Good to Be True Offers
- ✍️ Poor Grammar and Spelling Errors
- 📧 Suspicious Email Addresses and Links
- 🔐 Requests for Personal or Sensitive Information

Common Types of Phishing

EMAIL PHISHING

Phishing emails mimic real domains to trick users into clicking links, downloading malware, or giving personal data.

SPEAR PHISHING

Spear phishing targets specific people using known personal info to trick them into tasks like transferring money.

WHALING

Whaling targets top execs like CEOs, after detailed profiling to steal credentials due to their access to critical data.

SMISHING AND VISHING

Smishing uses fake SMS, while vishing uses calls to trick users into sharing personal or payment details with attackers.

ANGLER PHISHING

Fake social media accounts mimic brands to trick users into sharing data or clicking malicious links for support scams.

Essential Tips to Stay Secure from Phishing:

✅ **Verify the Sender's Email Address**
Always double-check the sender's email, especially the domain. Attackers often use slight variations of legitimate addresses to trick users (e.g., support@paypa1.com instead of support@paypal.com).

✅ **Hover Over Links Before Clicking**
Never click blindly. Hover over links to check the actual URL before clicking. If something looks off, go directly to the official website via browser.

✅ **Beware of Urgent or Threatening Messages**
Phishing emails often create a false sense of urgency (e.g., "Your account will be blocked!"). Pause, assess, and verify before taking action.

✅ **Look for Personalization**
Legitimate emails usually address you by name or title. Generic greetings like "Dear user" or "Dear customer" can be red flags.

✅ **Check for Branding & Professional Language**
Verify the presence of authentic branding, logos, and signatures. Also, look out for poor grammar or spelling errors — a common sign of phishing.

✅ **Avoid Sharing Sensitive Information Over Email**
Never share passwords, credit card numbers, or other sensitive data via email, even if the sender seems trustworthy.

✅ **Enable Two-Factor Authentication (2FA)**
Add an extra layer of protection to your social accounts. With 2FA, even if a password is compromised, attackers still need a second verification factor.

✅ **Keep Your Software & Browsers Updated**
Regularly update your operating system, browser, and antivirus tools to fix vulnerabilities that attackers often exploit in phishing campaigns.

✅ **Use Spam Filters and Secure Email Gateways**
Ensure that your email service or organization uses advanced spam filters and secure gateways that block malicious content before it reaches your inbox.

✅ **When in Doubt—Verify the Message**
If an email seems suspicious, contact the sender directly using known contact information (not by replying to the email). A quick call or message can clarify legitimacy.

Stay Sharp, Stay Secure

“The weakest link in cybersecurity isn’t the technology — it’s the human.”

In Conclusion:

Phishing is constantly evolving, but so can we. This campaign was a wake-up call — a reminder that even the most convincing emails can be traps. Together, we’ve taken the first step in building a stronger security culture. Awareness is the best defense.

What You Can Do Next:

- Report suspicious emails immediately.
- Complete the upcoming phishing awareness training.
- Encourage peers to stay cautious.
- Make cybersecurity a habit — not a one-time action.

Think Before You Click

Phishing threats are only a click away. Stay vigilant, report suspicious messages, and help keep our organization secure—because cybersecurity is everyone’s responsibility.