NOVENTIQ
Global AI Solutions

⚠ THINK BEFORE YOU CLICK

Phishing Awareness Guide

Spot the Red Flags

Unexpected request	"Your salary details have been updated. Review immediately."
Urgency or pressure	"Action required today." Messages designed to make you act before you think.
Suspicious link	The visible text may look legitimate, while the actual destination leads somewhere unexpected.
Unusual sender	The display name may look familiar, but the real email address may not belong to your organization.
Sensitive information	Requests for passwords, OTPs, MFA codes, bank details or other confidential information.
Too good — or too alarming	Unexpected rewards, threats, account suspension, payment demands or other emotional triggers.

Check Before You Trust

1. Check the sender **Look at the actual email address — not just the display name. A familiar name can be spoofed or imitated.**	**2. Hover over links** **Before clicking, hover over the link and inspect the destination. Be cautious of unfamiliar, misspelled or unrelated domains.**
3. Don't trust the logo **Branding, logos, signatures and professional formatting can all be copied. A convincing appearance does not prove an email is genuine.**	**4. Verify independently** **If a request seems unusual, confirm it through a trusted channel. Don't use contact details supplied in a suspicious message.**

Example: HR & Payroll Team <hr@company.com> ✓ vs. HR & Payroll Team <hr-payroll@random-domain.com>

What Can Happen After You Click?

A phishing page may ask you to sign in, enter your password, provide an OTP/MFA code, download a file, share personal information, or make a payment. Stop if an unexpected page asks for sensitive information.

Already clicked? Don't panic.

1. Don't enter credentials or sensitive information.
2. Close the suspicious page.
3. Report the email using your organization's approved phishing/reporting mechanism.
4. If you entered a password, follow your organization's password-reset/security procedure immediately.
5. If you downloaded something or shared sensitive information, contact IT/Security promptly.

The 10-Second Phishing Check

S — SENDER **Who actually sent this?**	**T — TARGET** **What is this email asking me to do?**
O — OPEN LINK **Where does the link really go?**	**P — PRESSURE** **Is the message trying to rush or scare me?**

NOVENTIQ
Global AI Solutions

STOP → LOOK → THINK. If something feels wrong, don't click. Verify first.

YOUR PHISHING SAFETY GUIDE

Simple habits that help protect you, your colleagues and the organization.

Before clicking an unexpected link or attachment

Pause. Don't let urgency make the decision for you.

Inspect. Check the sender, wording, link and attachment.

Verify. Confirm unusual requests through a trusted channel.

Protect. Never share passwords, OTPs or MFA codes because an email asks for them.

Report. When in doubt, use your organization's approved reporting process.

Remember

You weren't caught — you just got a chance to practice.

Phishing attacks often rely on one moment of trust. Taking a few seconds to stop and check can make all the difference.

Think before you click. Verify before you trust. Report when in doubt.

Security is everyone's responsibility.