LureSight

User Guide

How to spot dangerous emails — written for people who don't "do computers"

> **Read this first**
>
> You do not need to know anything about computers to use LureSight. If you can open an email and click a button, you can use everything in this guide.
>
> Any word that sounds technical is explained the first time it appears, and there is a small dictionary on the last page.

What is LureSight, in plain words?

"Phishing" (pronounced exactly like *fishing*) is when a criminal sends you a fake email that pretends to be from a real company — your bank, a delivery service, even your own boss. The goal is to trick you into clicking a bad link, typing in a password, or sending money.

LureSight is a small helper that lives inside Outlook, your email program. When you ask it to, it reads the email that is open on your screen and **points at the exact words and links that look suspicious**, with a short explanation of why. Think of it as a friend who reads over your shoulder and says, "Hmm, that part looks fishy — here's why."

> **Good to know**
>
> LureSight does its checking right on your screen. It does not send your emails to anyone, and nobody reads your mail. The only time anything is sent anywhere is when you press the "Report to security" button yourself.

Opening LureSight

1. Open the email you're unsure about, just like you normally read email.

2. Look at the strip of buttons near the top of the email. Find the one called **LureSight** or **Scan for phishing**. (On some screens it hides behind a button with three dots "…" — click the dots and you'll see it in the list.)
3. Click it. A panel slides in from the right side of your screen. That panel is LureSight.
4. Wait a moment while it says "Reading message…". The results appear on their own.

If you can't find the button at all, LureSight may not be installed yet — that's what the *Install Guide* (the other document that came with this one) is for.

Understanding what you see

1. The dial and the score

At the top of the panel is a half-circle dial with a number from 0 to 100. The higher the number, the more suspicious the email. Next to it is a plain-words verdict, and under that one short sentence saying the main reason — for example "Likely phishing — Hidden text written for an AI assistant, not for you." The verdicts are:

What it says	What it means	What you should do
Likely phishing	Many strong warning signs.	Don't click anything. Report it (see below), then delete it.
Suspicious	Several things don't look right.	Be very careful. When in doubt, report it and ask before acting.
Minor flags	One or two small oddities.	Probably fine, but read with your eyes open.
No obvious flags	Nothing suspicious was found.	Still use normal caution — see "An important honest note" below.

2. The highlighted copy of the email

Further down, LureSight shows a **copy** of the email with the suspicious parts colored in, like someone went over it with highlighter pens:

Highlight color	How worried to be
Red	Serious warning sign — for example, a link that says one address but secretly goes somewhere else.
Orange	Classic trickery — pressure like "act within 24 hours" or promises of prizes

Highlight color	How worried to be
	and refunds.
Yellow-green	A small oddity — like “Dear customer” instead of your actual name.

Click (or tap) any highlighted part and a little black box appears explaining, in one or two sentences, why that exact part was flagged. For links, it also shows where the link *really* leads — which is often the most eye-opening part.

> **Safe to explore**
> In this copy of the email, the links are switched off on purpose. You can click a highlighted link to read about it without any risk of actually opening it.

3. “Sender authentication” — did it really come from them?

Every email says who it's from — but that “From” name can be faked, the same way anyone can write any return address on an envelope. Luckily, emails also carry hidden postmarks that are much harder to fake. LureSight checks those postmarks for you.

Below the copy of the email is a line that says Details for your security team. Click it and a longer list opens: Sender authentication (headers), Sender, and Why it was flagged. You can ignore all of it — it is there for the people you report to — but the first part is worth a glance. Sender authentication lists what those checks found in plain language — for example, “the message failed sender authentication for the claimed domain.” You don't need to understand the details. The rule of thumb: anything marked HIGH in that section means the email very possibly did not come from who it claims.

4. The yellow banner on the email itself

After a scan finds problems, LureSight also places a warning strip on the email itself, so if you come back to that email tomorrow, the warning is still there reminding you.

5. Attachments are read too

If the email carries a PDF, LureSight reads the words and the links inside it, on your device, and checks them the same way as the rest of the email. If the PDF is locked with a password that is printed in the email itself, that is a warning sign on its own: real senders do not leave the key taped to the lock.

6. “Hidden text written for an AI assistant”

Some emails now carry writing you cannot see — white letters on a white background, or letters shrunk to nothing. It is not meant for you at all. It is written for the computer helpers that summarize email

(Copilot is one), and it tells them to describe the email as safe and routine, so that the short summary you read is the lie.

LureSight does not use that kind of helper, so the trick does not work on it. When it finds this, it says so at the top of the panel and shows you the hidden words inside the copy of the email, so you can read exactly what was planted. Treat the email as phishing, and do not trust any summary your email program showed you for it.

7. “Paste a command” instructions

A newer trick has no link to click and no file to open. The email, or the web page it sends you to, says something like “to prove you are human, press the Windows key and R, then press Ctrl and V, then press Enter.” A button on the page has quietly put a command on your clipboard. When you paste it and press Enter, you are the one who runs the criminal's program.

LureSight flags these instructions when they appear in an email, an attachment or a text message. But the rule is worth knowing by heart, because the same instruction can appear on a web page where LureSight cannot see it: no real company ever checks who you are, fixes an error or handles a complaint by asking you to paste something and press Enter.

8. Pages that were built in minutes

Fake sign-in pages and “appeal centers” used to look rough. Today a criminal can describe one in a sentence and a website-building tool produces a polished, working page, or they simply use a free online form. LureSight tells you when a message about your account, a payment or an appeal sends you to a page on one of these tools instead of to the company's own website.

You can check this yourself. Look at the web address before you type anything. A company deals with your account on its own address, such as yourbank.com. It does not send you to a page whose address ends in the name of a website builder, and it never asks for your password in a form.

Reporting a suspicious email

Reporting sends the email to the security team at your organization — the people whose whole job is dealing with this. Reporting is **always the right move** when something feels off. Nobody will be annoyed; they genuinely want these reports.

1. In the LureSight panel, click the blue **Report to security** button.
2. The very first time, it asks for the email address reports should go to. Type the address your IT or security team gave you (it often looks like *phishing@yourcompany.com*). You only do this once — it remembers.

3. A new email opens, already filled in: the address, a subject line, a summary of everything LureSight found, and the suspicious email attached. You don't have to write anything.
4. **Click Send.** That's it. You can now delete the suspicious email.

Made a mistake typing the address? Click the small ⚙ (gear) button next to “Report to security” to change it any time.

If your organization has set the reporting address for everyone, the gear button is not shown and the first-time question is skipped — the address is already right.

What should I do if...

- **...the score is high?** Don't click any links, don't open attachments, don't reply, and don't call phone numbers written in the email. Report it, then delete it.
- **...it looks like it's from my boss asking for a quick favor?** This is one of the most common scams. Check with them in person or by phone — using a number you already have, not one from the email.
- **...I already clicked a link or typed my password?** Don't panic, and don't hide it — speed matters far more than embarrassment. Tell your IT or security team right away and change that password.
- **...LureSight says the email is fine but my gut says otherwise?** Trust your gut and report it anyway. You are allowed to be more suspicious than the tool.
- **...the panel says the email has hidden text for an AI assistant?** Treat it as phishing. Whatever summary Outlook or Copilot showed you for that email was the target of the trick, so do not rely on it. Report the email and delete it.
- **...an email or a web page tells me to press some keys and paste something?** Stop. Do not press the keys. Close the page or the email, and report it. If you already pasted and pressed Enter, tell your IT or security team straight away and stop using that computer until they have looked at it.

An important honest note

LureSight is a helper, not a fortune-teller. Sometimes it flags an innocent email (newsletters love urgent-sounding language), and sometimes a clever fake slips past it. **A score of zero means “nothing suspicious was found,” not “this email is guaranteed safe.”** Your own judgment is still part of the team.

> **The three golden rules (worth more than any tool)**
> 1. Unexpected + urgent = suspicious. Real companies rarely demand action “within 24 hours.”
> 2. No legitimate company asks for your password by email. Ever.

3. When unsure, don't use anything in the email — no links, no phone numbers. Go to the company's website yourself or call a number you already know.

Little dictionary

Word	What it actually means
Phishing	A fake email designed to trick you into giving away information or money.
Add-in	A small extra feature you add to a program — like installing an app on your phone, but inside Outlook.
Link	Text you can click that opens a web page. The words shown and the place it opens can be different — that's the classic trick.
Attachment	A file that rides along with an email, like a photo or document clipped to a letter.
Spam	Junk advertising. Annoying but usually harmless. Phishing is the dangerous cousin.
Domain	The part of a web or email address after the @ or www — like “yourbank.com.” Crooks use lookalikes such as “yourbank-secure.com.”
IT / security team	The people at your organization who look after computers and safety. The ones who receive your reports.
AI assistant / Copilot	A computer helper that can read your emails and write a short summary of them. Handy, but it can be fooled by hidden writing — see section 6.
Hidden text	Words in an email that are invisible to you (white on white, or tiny) but are still there in the email's code. Crooks use it to talk to AI assistants behind your back; LureSight shows it to you.
PDF	A common kind of document file, often used for invoices and statements. LureSight reads the words and links inside PDFs that come with an email.