Cyber Suite

montimage

Uptake of Innovative Security-as-a-Service Solutions

Detecting Phishing Attacks & Competing in Training Challenges

Instructor: Edgardo Montes de Oca

Montimage

Co-funded by the European Union

Co-Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or Digital Europe Programme. Neither the European Union nor Digital Europe Programme can be held responsible for them.

Agenda

01 Course Introduction

02 Module 1: Getting Started

03 Module 2: Training Mode

04 Course Wrap-Up and Evaluation

Course Introduction

An **interactive platform** that teaches you to **identify phishing emails** through **progressive levels**, **real-time AI feedback**, and **gamified challenges**.

Why phishing awareness matters

- Phishing is the most common entry point for cyberattacks — it targets people, not just systems.
- Attackers exploit trust, authority, urgency, fear and curiosity to trick you into clicking or replying.
- A single successful phishing email can lead to stolen credentials, fraud, or malware.
- Technical filters help, but the human eye is the last line of defense — and it can be trained.

This course trains that skill through **realistic, hands-on practice**.

What you will learn

- Understand **what phishing is** and **how email phishing attacks work**
- Recognize the **common types** of phishing attacks
- Apply a repeatable checklist to **identify suspicious emails**
- Train through **4 progressive difficulty levels** with real-time AI feedback
- Track your **progress** and improve your **detection accuracy**
- Join **challenges & hackathons** and earn **badges and certificates**

Who this course is for

This course is for **anyone who uses email and wants to spot phishing**: corporate employees, students, and individual learners.

No security background is required — every concept is introduced from the ground up. It is also useful for teams preparing for phishing-awareness challenges and hackathons.

<2 hrs
self-paced

How the course is structured

The course is organised as five short modules. Each module is a brief lesson, and the full effort is under 2 hours, self-paced.

Module	Topic	Estimated Time
1	Getting Started and Understanding Phishing Attacks	1 hour
2	Training Mode	1 hour

You can follow the course at your own pace; the full effort is under **2 hours**.

Recommended procedure to follow

1. Watch the short demo video for each module (or read this deck).
2. Open the platform at pdtp.montimage.eu and follow along.
3. If a term or concept is unclear, use the in-app Help Center or search the web.
4. Practise in Training Mode until the checks feel natural, then join a challenge.
5. At the end, share your feedback so we can improve the course.

Hands-on: try the platform

The platform is **web-based at pdtp.montimage.eu**, with 4 short demo videos covering Sign-up & register, Training Mode, Tracking Progress, and Challenge Mode.

Goals: follow along with each video, then practise on the platform to build your phishing-detection skills.

Link:
https://www.youtube.com/playlist?list=PLVYNqtl4p3e0pUQ5p38uW0PynTLphSSNG

SCAN ME!

Module 1: Getting Started

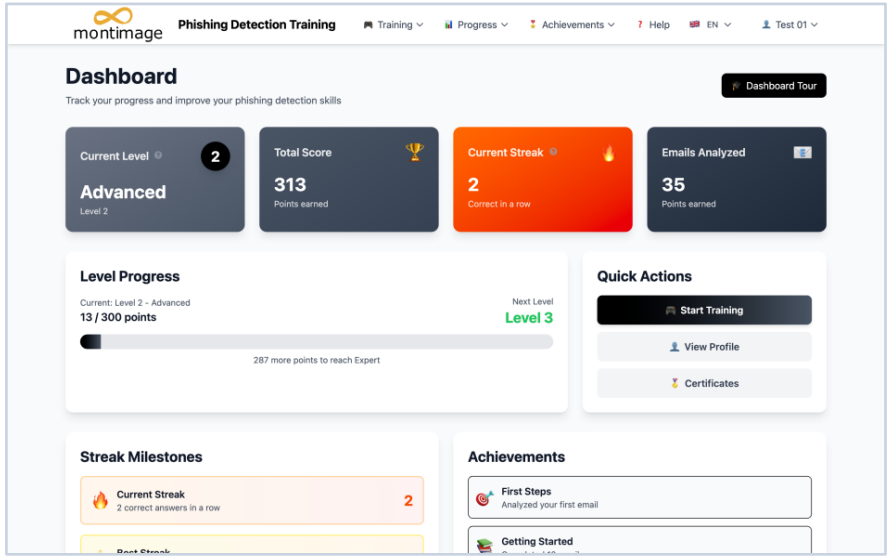
- Create an account and sign in (Email/Password or Google)
- Set your preferred language
- Find your way around the dashboard
- Know where to see your progress and profile

Watch the demo:
Sign up & register

Create your account & get oriented

Getting started takes just a minute. The platform is web-based — no install required.

- Sign up with Email/Password or Google, then sign in
- Available in 5 languages: English, French, Greek, Spanish, Dutch
- The dashboard is your home base: training, challenges, progress and profile
- Update your details anytime in Settings and Profile



Tip: log in to unlock your full progress, badges and certificates.

Understanding Phishing Attacks

- Define phishing and explain why it works
- Describe the anatomy of an email phishing attack
- Recognize the 10 common attack types
- Apply a 6-point checklist to identify phishing emails
- Rate the severity of a threat using risk levels

What is phishing?

Phishing is a form of social engineering — it attacks the person, not the machine, tricking you into clicking, replying, or handing over information.

- It exploits emotional triggers: authority, urgency, fear, curiosity and greed
- The goal: steal credentials or money, deliver malware, or gain access
- Email phishing is the most common form
- The same trick appears as smishing (SMS), vishing (voice) and quishing (QR codes)

Because phishing targets human judgement rather than technology, no filter catches everything. Learning to recognise the triggers and tricks is your strongest line of defence — and exactly what this platform trains.

Anatomy of an email phishing attack

Attackers follow a repeatable kill chain:

Target → Lure → Hook → Payload → Exploit.

- **Sender** — spoofed or lookalike addresses
- **Subject** — bait designed to make you open it
- **Body** — the persuasive message and its request
- **Links** — where a click really goes (hover to reveal)
- **Attachments** — files that carry the payload

Popular types of phishing attacks

Attack Type	What it is	Example giveaway
Spear Phishing	Targeted, researched attack on one person	Email using your real name & role
Credential Harvesting	Fake login page to steal passwords	“Confirm your password” link
Business Email Compromise	Impersonates an exec to authorise fraud	“CEO” asks for an urgent transfer
Malware Delivery	Attachment/link installs malware	Unexpected invoice.zip
Social Engineering	Pure psychological manipulation	“I need a favor, keep this quiet”
Invoice / Payment Fraud	Fake bill or changed bank details	Vendor “updated” their IBAN
Account Takeover	Lures aimed at hijacking access	“Unusual login — verify now”
Spam / Unsolicited	Bulk unwanted mail; a delivery vector	Mass marketing blast
Scam / Fraudulent Offer	Too-good-to-be-true offers	Lottery / advance-fee
Brand / Executive Impersonation	Spoofs a trusted brand or leader	Fake “Microsoft” security alert

How to identify a phishing email

1. Sender — mismatched or lookalike domains, display-name spoofing
2. Content — poor grammar, generic greetings, off-context requests
3. Link — hover to reveal; URL mismatch, shorteners, misspelled domains
4. Attachment — unexpected files; risky types (.exe, .zip, .html)
5. Urgency — pressure, deadlines, threats, “act now”
6. Social Engineering — authority/trust/fear cues; what is really being asked

These 6 areas are exactly the skills the platform scores.

Rate the severity: 5 risk levels

Don’t just spot the flag — judge how dangerous it is. The platform uses five risk levels:

Very Low → Low → Medium → High → Critical

- Credential theft, payment fraud and malware are usually High or Critical
- Unsolicited spam with no request is usually Low
- Assigning a risk level is part of Level 3 classification

From theory to the 4 training levels

- Level 0 — Phishing or legitimate? The core yes/no judgement
- Level 1 — Spot the suspicious element (sender, subject, body, etc.)
- Level 2 — Explain the threat with detailed reasoning
- Level 3 — Classify the attack type and assess its risk level

Everything you learned in this module is what you practise next.

Hands-on: spot the phish

1. Open pdtp.montimage.eu and start a Level 0 session.
2. For each email, decide: phishing or legitimate?
3. Read the AI feedback and note which red flag you missed.
4. Move up to Level 1 and identify the suspicious element.
5. Compare your reasoning to the 6-point checklist.

Summary

- Phishing is social engineering — it targets people using authority, urgency and fear.
- An email phishing attack follows a kill chain and abuses the sender, subject, body, links and attachments.
- There are 10 common attack types, from spear phishing to impersonation.
- A 6-point checklist plus a 5-level risk scale lets you identify and rate any suspicious email.

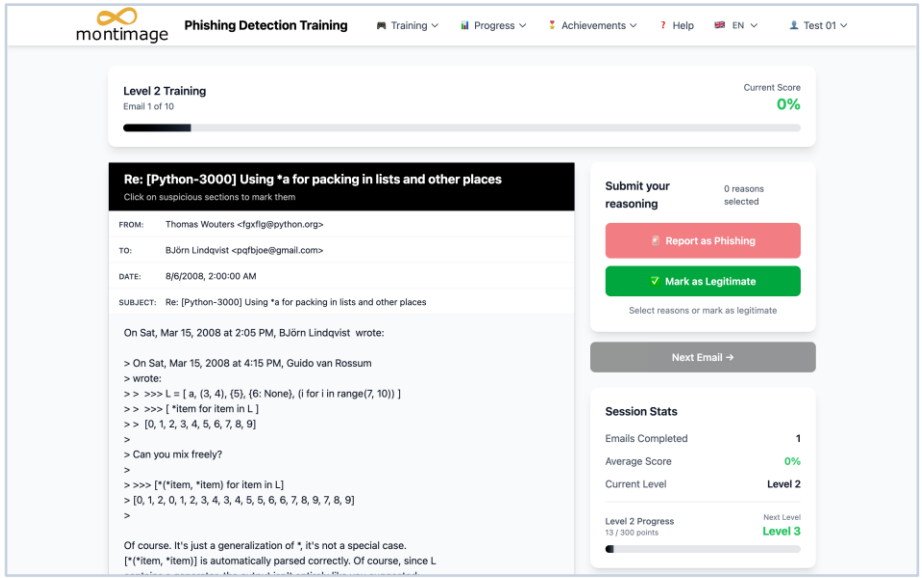
Module 2: Training Mode

- Start and complete a training session
- Switch between the 6 email-client themes
- Read real-time AI feedback
- Understand the difference between score and accuracy

How a training session works

Training Mode is where you practise everything from Module 1 and get instant feedback.

- Start from the lobby, pick your difficulty level, and begin
- Emails render in 6 realistic client themes: Outlook, Gmail, macOS Mail, Thunderbird, iOS Mail, ProtonMail
- After each answer, real-time AI feedback explains what you missed
- A collapsible side-by-side view compares the email against the feedback
- Emails are shuffled so every session stays realistic



Score vs. accuracy

Training Mode reports a score and an accuracy rate, plus feedback on every answer. The table explains each one.

Chase both — a high score with low accuracy means volume, not mastery.

Metric	What it measures
Score	Points earned — rewards correct, confident and fast answers
Accuracy	The percentage of your answers that were correct
Feedback	The AI explanation of the right answer and why

Hands-on: play a full session

1. Start a training session at your current level.
2. Classify at least 10 emails.
3. Read the AI feedback after every answer.
4. Open your session summary and note your score and accuracy.
5. Switch to a different email-client theme and repeat.

Summary

- Training Mode lets you practise phishing detection with instant AI feedback.
- Emails appear in 6 realistic client themes and in shuffled order.
- Score rewards correct, confident, fast answers; accuracy measures how often you are right.
- Aim to raise both your score and your accuracy as you climb the levels.

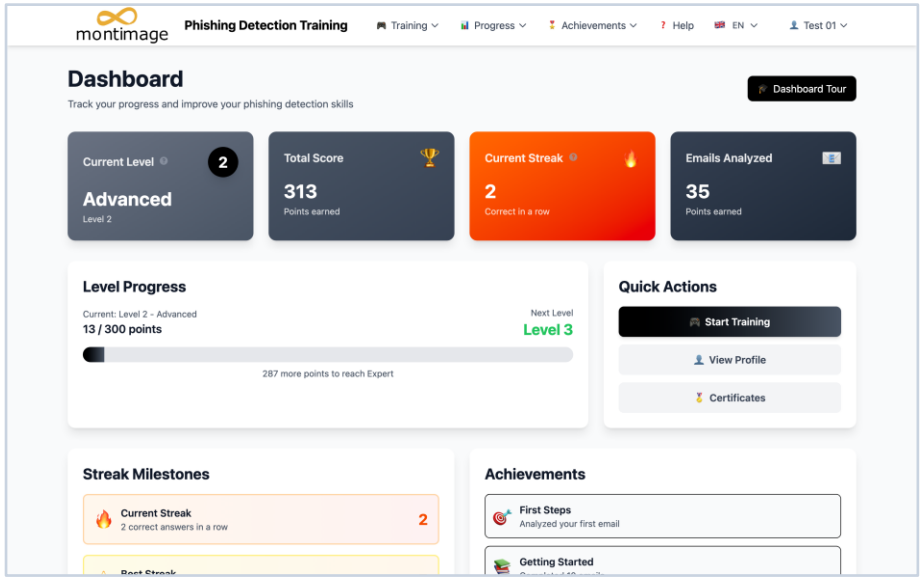
Tracking Your Progress

- Read your session statistics and accuracy rates
- Understand your per-skill proficiency
- Find and use your assessment reports
- Decide what to work on next

Your dashboard & reports

Your progress turns into a plan — the dashboard shows where you are strong and where to improve.

- Session statistics: totals, trends and history across all your training
- Accuracy rates: how reliably you classify emails over time
- Skill proficiency: your strength across the 6 detection skill areas
- Assessment reports: downloadable PDF / Markdown summaries of your results



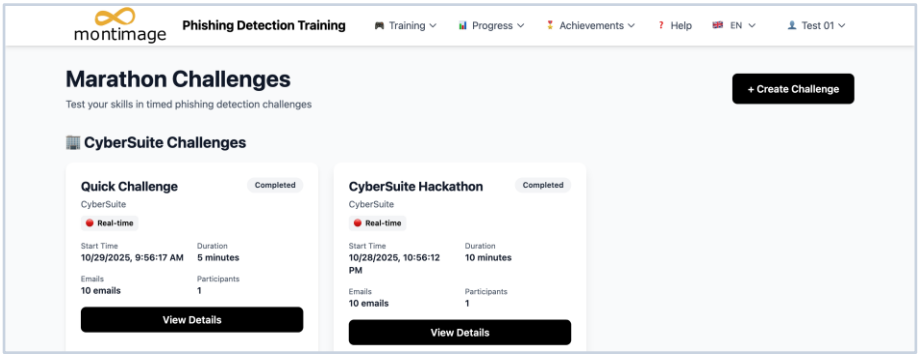
Extra Features

- Discover the platform’s competitive and motivational features
- Join challenges and hackathons
- Earn badges and certificates
- Climb the leaderboards

Extra feature: Challenges & hackathons

Beyond solo training, you can compete against others in timed challenges.

- Browse open challenges and register before kick-off
- Play a live challenge against the clock, with color-coded countdown timers
- Challenges range from 5 to 50 emails and can be public or organization-only
- Challenges auto-complete on timeout — and you can spectate live ones

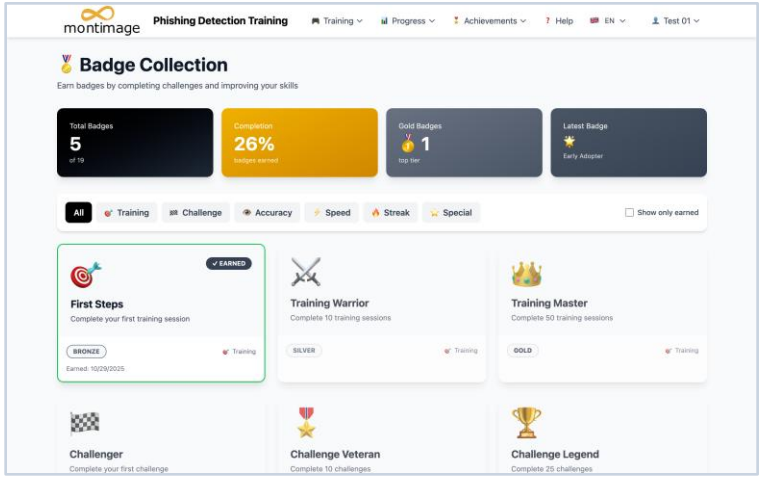


Challenges turn practice into **friendly competition**.

Extra features: Badges, certificates & leaderboard

The platform rewards steady progress and lets you prove your skills.

- Badges: 18 badges across 6 categories (Training, Challenge, Accuracy, Speed, Streak, Special) and 4 tiers
- Certificates: 6 levels from Newbie to Legend, with public verification and 365-day validity
- Leaderboards: compare globally or within your organization, with medals for top-3 finishes
- Together they keep training engaging and give you something to show for it



Course Wrap-Up and Evaluation

Congratulations on completing the **Phishing Detection Training Platform course**!

What you learned from this course

- **Understand what phishing is** and why it works.
- **Recognize the common types of phishing attacks**.
- **Apply a 6-point checklist** to identify suspicious emails and rate their risk.
- **Train through 4 progressive levels** with real-time AI feedback.
- **Track your progress** and improve your detection accuracy.
- **Compete in challenges** and earn badges and certificates.

We Value Your Feedback!

Please take a few minutes to complete our short course-evaluation survey. Your honest feedback helps us improve the lessons, labs, and the platform itself for future learners.

What the survey asks about

- The clarity and usefulness of each module.
- Whether the hands-on labs were easy to follow and worked as expected.
- The pacing and overall difficulty of the course.
- Any technical issues you encountered with the platform.
- Suggestions and features you would like to see.

Take the survey

Please complete the evaluation form. The survey is anonymous and takes about five minutes. Thank you for helping us make the course better and good luck applying your new phishing detection skills to stay safe against real-world attacks.

Thank you for your attention!

Montimage

Edgardo Montes de Oca, Manh Nguyen

luong.nguyen@montimage.eu
edgardo.montesdeoca@montimage.eu

https://www.pdtp.montimage.eu

Co-funded by the European Union

Co-Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or Digital Europe Programme. Neither the European Union nor Digital Europe Programme can be held responsible for them.