Slide 1

Hello, and welcome everyone to this course, “Uptake of Innovative Security-as-a-Service Solutions – Detecting Phishing Attacks and Competing in Training Challenges.”

My name is Edgardo Montes de Oca, from Montimage.

I will be guiding you through this curriculum. This course is part of the CyberSuite project, which is co-funded by the European Union and focuses on implementing innovative Security-as-a-Service solutions to protect modern digital infrastructures. In this course, we turn our attention to the most common way attackers get in – phishing – and to the interactive platform that trains you to spot it.

Slide 2

Here is how our journey is organized.

We will begin with a short course introduction, and then move into Module 1, where you get started as a participant – creating your account and finding your way around.

This is followed by an explanation of what phishing attacks are and how to recognize them.

In Module 2, you will play a training session and learn how the platform gives you feedback, and how to track your progress over time.

Extra features are also presented including the challenges, badges, certificates, and leaderboards – that make the training competitive and rewarding.

We finish with a course wrap-up and an evaluation.

Slide 3

Let’s start with the course introduction.

The Phishing Detection Training Platform is an interactive platform that teaches you to identify phishing emails. It does this through progressive difficulty levels, real-time AI feedback on every answer, and gamified challenges that keep the practice engaging.

Slide 4

To understand why this skill matters, let’s look at the problem.

Phishing is the most common entry point for cyberattacks – and what makes it so effective is that it targets people, not just systems.

Attackers exploit human instincts: trust, authority, urgency, fear, and curiosity, to trick you into clicking a link or replying with information. A single successful phishing email can lead to stolen credentials, financial fraud, or malware on your device.

Technical filters help, but they never catch everything. The human eye is the last line of defense – and, unlike a filter, it can be trained. That is exactly what this course does, through realistic, hands-on practice.

Slide 5

By the end of this course, you will have a well-rounded set of skills.

You will understand what phishing is and how email phishing attacks actually work. You will be able to recognize the common types of phishing attacks, and apply a repeatable checklist to identify suspicious emails.

You will train through four progressive difficulty levels, each with real-time AI feedback, and you will learn to track your own progress and steadily improve your detection accuracy.

Finally, you will discover how to join challenges and hackathons, and earn badges and certificates that recognize and prove your skill.

Slide 6

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

No security background is required. Every concept is introduced from the ground up, so you can follow along whether or not you have any prior experience. The course is also useful for teams preparing for phishing-awareness challenges and hackathons.

Slide 7

The curriculum is built for flexibility. It is organized as 2 modules, and the full effort is under three hours, entirely self-paced.

Getting started and understanding phishing attacks takes about an hour.

The training mode, tracking your progress and the extra features about one hour.

You can take the course at your own pace and continue using the phishing detection game to practice spotting fraudulent emails quickly.

Slide 8

Here is the recommended procedure to get the most out of the course.

For each module, watch the short demo video – or simply read through this deck. Open the platform at pdtp.montimage.eu and follow along as you go.

If a term or concept is unclear, pause and use the in-app Help Center, or search the web for more detail. Active participation is important for building real skill.

Practise in Training Mode until the checks feel natural, and then join a challenge. And at the end, please share your feedback – this is important for us to be able to improve the course.

Slide 9

Practical application is at the heart of this course.

The platform is web-based, at pdtp.montimage.eu, with no installation required. Alongside it, there are four short demo videos covering sign-up and registration, Training Mode, tracking your progress, and Challenge Mode.

Your goal is to follow along with each video, and then practise on the platform yourself to build your phishing-detection skills. You can reach the full demo playlist by scanning the QR code on this slide, or using the link provided.

Slide 10

We now begin Module 1, Getting Started as a Participant and understanding phishing attacks.

In this lesson, you will create an account and sign in – either with an email and password, or with your Google account. You will set your preferred language, find your way around the dashboard, and learn where to see your progress and your profile.

To follow along, watch the demo video: Sign up and register.

Slide 11

Getting started takes just a minute, and because the platform is web-based, there is nothing to install.

You sign up with an email and password, or with Google, and then sign in. The platform is available in five languages – English, French, Greek, Spanish, and Dutch – so you can work in whichever you're most comfortable with.

Once you're in, the dashboard is your home base: it brings together your training, your challenges, your progress, and your profile. You can update your details at any time in the Settings and Profile pages.

One tip: be sure to log in, rather than just exploring anonymously, so that the platform can save your full progress, badges, and certificates.

Slide 12

First of all, it is important to understand what phishing attacks are. We address this topic here so that you can recognize actual attacks when they occur.

We define what phishing is and explain why it works. You will describe the anatomy of an email phishing attack, recognize the ten common attack types, apply a six-point checklist to identify phishing emails, and learn to rate the severity of a threat using risk levels.

Slide 13

So, what is phishing?

Phishing is a form of social engineering. That means it attacks the person, not the machine – tricking you into clicking, replying, or handing over information. It works by exploiting emotional triggers: authority, urgency, fear, curiosity, and greed.

The attacker's goal is usually to steal your credentials or money, to deliver malware, or to gain access to a system. Email phishing is the most common form, but the very same trick also appears as smishing over SMS, vishing over voice calls, and quishing through QR codes.

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

Slide 14

It helps to understand how an attacker actually builds a phishing email, because they tend to follow a repeatable kill chain: target, lure, hook, payload, and exploit.

Within the email itself, there are a handful of parts the attacker controls and abuses. The sender is often a spoofed or lookalike address. The subject is bait, designed to make you open the message. The body carries the persuasive message and its request.

Then there are the links – where a click really goes, which you can reveal by hovering – and the attachments, which are the files that carry the payload. These are exactly the parts you'll learn to inspect in the platform.

Slide 15

Phishing comes in several recognizable types, and the platform scores you on ten of them.

Spear phishing is a targeted, researched attack on one specific person – for example, an email that uses your real name and job role. Credential harvesting uses a fake login page to steal your password, often behind a "confirm your password" link. Business Email Compromise impersonates an executive to authorize fraud – the classic "CEO" asking for an urgent transfer. Malware delivery hides its payload in an attachment or link, like an unexpected invoice.zip.

Social engineering is pure psychological manipulation – "I need a favor, keep this quiet." Invoice or payment fraud uses a fake bill or changed bank details, such as a vendor that suddenly "updated" its IBAN. Account takeover lures aim to hijack access with "unusual login – verify now" messages. Spam is bulk unwanted mail, a lower-risk but real delivery vector. Scams are too-good-to-be-true offers, like a lottery or advance-fee. And brand or executive impersonation spoofs a trusted brand or leader – think of a fake "Microsoft" security alert.

Slide 16

To catch these attacks reliably, you want a repeatable inspection routine. The platform organizes it into six areas – the same six skills it scores you on.

Check the sender for mismatched or lookalike domains and display-name spoofing. Check the content for poor grammar, generic greetings, and off-context requests. Check each link by hovering to reveal it, watching for URL mismatches, shorteners, and misspelled domains. Check attachments for unexpected files and risky types like .exe, .zip, or .html.

Then look at urgency – pressure, deadlines, threats, and “act now” language – and at the underlying social engineering: the authority, trust, or fear cues, and what the message is really asking you to do.

Slide 17

Spotting a red flag is only half the job. You also need to judge how dangerous it is.

The platform uses five risk levels, from Very Low, to Low, to Medium, to High, and finally Critical.

As a rule of thumb, credential theft, payment fraud, and malware are usually High or Critical, because the consequences are severe. Unsolicited spam with no real request is usually Low. Assigning a risk level like this is part of what the platform calls Level 3 classification.

Slide 18

Everything in this module maps directly onto the four progressive training levels you’ll practise next.

Level 0 is the core yes-or-no judgement: is this email phishing, or legitimate? Level 1 asks you to spot the suspicious element – the sender, the subject, the body, and so on. Level 2 asks you to explain the threat with detailed reasoning. And Level 3 asks you to classify the attack type and assess its risk level.

In other words, everything you have just learned in this module is exactly what you go on to practise.

Slide 19

Let’s put this into practice.

Open pdtp.montimage.eu and start a Level 0 session. For each email, make the core decision: phishing, or legitimate? Read the AI feedback after each one, and note which red flag you missed.

Then move up to Level 1 and identify the suspicious element in each email. As you go, compare your reasoning against the six-point checklist, so the theory and the practice reinforce each other.

Slide 20

To summarize : 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 ten common attack types, ranging from spear phishing to brand impersonation.

And with a six-point checklist plus a five-level risk scale, you can both identify and rate any suspicious email you encounter.

Slide 21

Now that you understand phishing in theory, Module 2, Training Mode, is where you put it into practice.

In this lesson, you will start and complete a training session, switch between the six email-client themes, read the real-time AI feedback, and understand the important difference between your score and your accuracy.

Slide 22

Training Mode is where you practise everything from Module 1 and get instant feedback on how you're doing.

You start from the lobby, pick your difficulty level, and begin. Each email is rendered in one of six realistic client themes – Outlook, Gmail, macOS Mail, Thunderbird, iOS Mail, and ProtonMail – so you learn to spot phishing in whatever interface you actually use.

After each answer, real-time AI feedback explains exactly what you missed, and a collapsible side-by-side view lets you compare the email against that feedback. The emails are shuffled every time, so no two sessions are quite the same and each one stays realistic.

Slide 23

Training Mode reports two numbers you should understand clearly: a score and an accuracy rate, plus feedback on every answer.

The score is the points you earn – it rewards answers that are correct, confident, and fast. Accuracy is simply the percentage of your answers that were correct. And the feedback is the AI's explanation of the right answer and why.

The key insight is to chase both. A high score with low accuracy just means you answered a lot of emails, not that you mastered them. Real progress shows up when your score and your accuracy rise together.

Slide 24

Now it’s your turn to play a full session.

Start a training session at your current level and classify at least ten emails. Read the AI feedback after every single answer – that’s where the learning happens.

When you finish, open your session summary and note both your score and your accuracy. Then switch to a different email-client theme and repeat, so you get comfortable spotting phishing across different interfaces.

Slide 25

Training Mode lets you practise phishing detection with instant AI feedback on every answer.

Emails appear in six realistic client themes and in shuffled order, so the practice always feels real. Remember that score rewards correct, confident, and fast answers, while accuracy measures how often you are right.

Your aim is to raise both your score and your accuracy as you climb through the levels.

Slide 26

Tracking Your Progress, is about turning your practice into a plan.

Here, you will learn to read your session statistics and accuracy rates, understand your proficiency across each skill area, find and use your assessment reports, and decide what to work on next.

Slide 27

Your progress data turns into a plan: the dashboard shows you where you are strong and where you can improve.

Session statistics give you the totals, trends, and history across all of your training. Accuracy rates show how reliably you classify emails over time. Skill proficiency breaks down your strength across the six detection skill areas, so you can see, for example, whether links or attachments are your weak spot.

And your assessment reports are downloadable PDF or Markdown summaries of your results – useful for reviewing your own progress, or sharing it. Use all of this to decide which level or which skill to focus on next.

Slide 28

Finally we provide a description of the platform's Extra Features – the competitive and motivational parts that make the training stick.

Here, you will discover how to join challenges and hackathons, how to earn badges and certificates, and how to climb the leaderboards.

Slide 29

Beyond solo training, the platform lets you compete against others in timed challenges.

You can browse the open challenges and register before kick-off. When a challenge goes live, you play against the clock, with color-coded countdown timers keeping the pressure on. Challenges range from five to fifty emails, and can be public or restricted to your organization.

If a challenge times out, it auto-completes for you, and you can even spectate live challenges to watch how others play. In short, challenges turn solo practice into friendly competition.

Slide 30

The platform also rewards steady progress and lets you prove your skills, through badges, certificates, and leaderboards.

There are eighteen badges, across six categories – Training, Challenge, Accuracy, Speed, Streak, and Special – and four tiers to work up through. Certificates come in six levels, from Newbie all the way to Legend; each one is publicly verifiable and valid for three hundred and sixty-five days. And the leaderboards let you compare yourself globally or within your own organization, with medals for top-three finishes.

Together, these features keep the training engaging, and give you something concrete to show for the skills you've built.

Slide 31

Congratulations on completing the Phishing Detection Training Platform course!

Let’s recap what you have learned. You now understand what phishing is and why it works, and you can recognize the common types of phishing attacks. You can apply a six-point checklist to identify suspicious emails and rate their risk.

You have trained through four progressive levels with real-time AI feedback, learned to track your progress and improve your detection accuracy, and seen how to compete in challenges and earn badges and certificates.

Slide 32

Before you go, we’d be grateful for your feedback.

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

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 ran into, and any suggestions or features you’d like to see.

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.

Slide 33

Thank you for your attention and hard work throughout this course.

If you have any further questions, or would like to learn more about our work, please reach out to us at Montimage using the contact information on this slide, or visit the platform at pdtp.montimage.eu.

Good luck, and stay safe out there!