Respondent A

Increased suspicious mail - Acknowledges not very often, but increasing frequency.

Company test mails - Awareness that the company sends its own test phishing emails.

Private mail vigilance - Experiences more suspicious emails on the private side, requires more alertness.

First reaction suspicious mail - First reaction to a suspicious email.

Identification by sender context - Identifies suspicious mail based on their work context (getting emails from foreign Y-companies when not working with them).

Identification by language quality - Identifies phishing by poor English quality in emails.

Not proper business english - Confirmation that the English is not professional business English.

Identification by link presence - Identifies suspicious emails when they always include a link to click.

Self-assessed knowledge - Rates current phishing knowledge as a two on a scale of one to five.

Need for more vigilance - Feels a need to become much more vigilant.

Past clicks acknowledged - Has clicked on some links that should not have been clicked (two times).

Experience - password reset scam - Clicked a link from an email appearing to be from the company about changing login, then changed login.

Experience - accidental re-click - Made a mistake by accidentally clicking a reported fake email that remained in the inbox.

Reported emails remain - Expresses frustration that reported emails remain in the inbox.

Desire auto-removal after report - Wishes reported emails would automatically disappear/be removed.

Reporting system generally good (except retention) - Thinks the reporting system (besides email retention) generally works well.

Dilemma - opening email - Acknowledges one must open the email to identify if it's fake, but opening is already a "mistake."

Training can help with identification - Suggests training and examples could help identify advanced fake emails.

Awareness of reporting methods - Only aware of the small report flag in Outlook.

Alternative reporting - call - Can call someone to ask about suspicious emails.

No manager spoofing received - Has not received fake emails from own managers yet.

Identification by link hover - Looks at the full email address by hovering the mouse over the link.

Comfort asking colleagues/managers - Feels comfortable asking colleagues or managers if uncertain.

Positive reinforcement of reporting (example) - Recalls an instance where an email was reported, then IT confirmed it was okay on the company website.

Better to avoid click than risk - Better to skip/delete suspicious emails than click.

Past training experience - Has not had specific phishing training before recently, but has had some information.

Recent company training - Recently (last week/May 2025) participated in short sequences and an avatar-based training.

Training certificates received - Received certificates for each training.

Phishing discussions in company - Phishing is discussed often in company conferences and meetings, "kept open."

Desire for practical skills - Wants practical knowledge to feel more self-assured in identifying phishing.

Fear of inspecting email - Hesitant to even open/click emails to inspect them due to fear of registration/consequences.

Desire for safe preview tool - Wishes for a tool to safely preview emails without opening/clicking them.

Training format preference (videos) - Prefers short videos for training.

Training language preference - Prefers training to be in Swedish due to difficulty understanding English terms.

Training repetition/practice - Wants to be able to practice immediately after learning and repeat training multiple times.

Training immediate feedback - Desires immediate feedback within training, showing where mistakes were made.

Training duration preference - Prefers shorter, more frequent training sessions over long, infrequent ones.

Continuous alertness benefit - Shorter, more frequent training keeps one alert.

Perceived colleague uncertainty - Believes many colleagues are also uncertain or don't know what to look for.

Training reminder format - Suggests email reminders for new training modules and fixed deadlines (2-3 weeks).

Threat evolution speed - Acknowledges threats evolve quickly, requiring frequent updates to training.

Training need - post-click protocol - Desires training on what to do if one has clicked a malicious link to minimize damage.

Immediate incident response - Wants a quick link/panic button for immediate help/action after clicking.

Panic button placement - Suggests panic button next to report button or other common Outlook features.

Respondent B

Some suspicious mail clear - Sometimes suspicious emails are clear.

Unnoticed passage of phishing - Believes many suspicious emails pass unnoticed.

High volume deletion - Deletes a huge volume of "X-mail" without reading.

Clear identification possible - In some cases, can clearly identify that an email is suspicious.

Identification by "click here" - Identifies by "click on..." or "can you answer this" prompts.

Identification by similar email address - Identifies by similar-looking email addresses that are not official.

Identification by manager spoofing - Recognizes "manager@blablabla" spoofs as suspicious.

Initial step - contact IT head - First step is to email IT head for guidance on how to handle the email.

Avoid forwarding without IT - Does not forward anything without informing IT.

Proactive reporting - Contacts IT when something needs to be "lifted" (reported).

Unreported deletions - Acknowledges probably deleting some suspicious emails without reporting them.

Self-assessed knowledge - Rates current phishing knowledge between 3 and 4 out of 5.

Skilled attackers deceive anyone - Believes everyone can be fooled by skilled attackers.

IT dept members fooled - Notes that even IT department members have sometimes clicked on suspicious items.

High caution/vigilance - Is very cautious and it would take a lot to click on something.

Preference: delete over risk - Prefers to delete an email if uncertain rather than open it.

Fooled by fake websites - Has been fooled by fake websites, but not necessarily clicked a direct link in an email.

Contextual vulnerability - rushed - Example of being deceived by a fake shopping site during Christmas rush, when rushed.

Learning from past mistakes - Once fooled, eyes are kept extra open.

General vigilance - Describes being very "om sig, kring mig" (aware of surroundings).

Children's critical thinking - Teaches children to be aware; notes they are schooled to be critical from a young age.

Hope for phishing decline - Hopes that increased critical thinking will make phishing disappear.

Generational susceptibility - Believes older generations were more susceptible to phishing.

Increased general awareness - Notes that many people are now more enlightened.

Comfort asking colleagues/managers - Feels quite comfortable asking colleagues/managers.

Past fear of asking - Acknowledges a past period where people were afraid to ask/feel dumb.

Asking for help is normal - Believes asking for help has become normalized.

Attackers are professional - Acknowledges attackers are professional criminals, using new techniques (AI).

Need for multiple eyes - Sometimes needs multiple eyes/opinions on suspicious emails.

Better to ask than be sure - Better to ask, as no one can be 100% sure.

Does not use Outlook report button - Has not used the standard Outlook "report" button.

Prefers screenshot to IT - Prefers sending emails as a screenshot and details directly to IT.

IT wants information - Acknowledges IT wants the information.

User desire to remove email - Wants to remove suspicious emails from inbox to prevent accidental clicks later.

Company has increased focus on cybersecurity training - Company has increased focus on cybersecurity training in last year.

Previous training was societal - Previous training was more "general societal information."

No specific training at early workplaces - No specific training at earlier workplaces.

Training formats - Training in various formats: meetings, conferences, digital training modules.

Desire for real-life examples - Prefers training that highlights different examples of how phishing can look.

Training format preference (gamification) - Believes gamification is a good way to learn; interactive scenarios.

Training behavioral practice - Gamification allows behavior to be trained simultaneously with learning.

Training continuity/red thread - Interactive modules need a "red thread" through different scenarios.

Learning through reflection - Believes doing interactive training leads to more reflection.

Training duration preference - Prefers shorter, more frequent training sessions for repetition.

Long training forgotten - Long training sessions are easily forgotten.

Training reminders - Prefers pop-up reminders for training.

Risk of dismissing reminders - Acknowledges risk of clicking away pop-ups and forgetting.

Varied reminder formats - Suggests varied formats like calendar reminders.

Digital exercises + physical meet - Suggests mixing digital exercises with physical meetings/workshops.

Feedback sessions importance - Importance of feedback sessions where participants can discuss and reflect.

Open discussion about vulnerability - Important to talk about being fooled to reduce stigma, normalize asking for help.

Situational vulnerability (stress) - More susceptible when stressed or in a hurry.

Training adaptation - Training should address language barriers and be adapted for different knowledge levels/roles.

Continuous dialogue - Importance of continuous dialogue about phishing to normalize it.

No blame culture - Important for people to feel they haven't done anything wrong.

Phishing - important topic - Considers phishing an interesting and super important topic.

Respondent C

Objective: lessen human factor risk - Primary objective is to lessen the risk of the human factor.

Human error is inevitable - "Someone will fall for a phishing attempt, period."

IT savvy can still fall - Even IT savvy people can fall for it.

Objective: provide recognition tools - To give people tools to recognize and be aware of phishing.

Phishing campaign use - Uses an active phishing campaign where people are "actively phished."

Main philosophy: repetition - The main philosophy is repetition to keep it "top of mind."

Training frequency - Training 4-5 times a year.

Training duration - Quick 5-10 minute trainings.

News posts for awareness - Uses news posts every now and then.

Objective: minimize risk - General idea is to minimize risk.

Technical tool: quarantine - Uses email quarantine.

Technical tool: defender - Uses standardized tools that Defender offers (email scanning/blocking).

Flagged email review - Flagged emails are reviewed by someone knowledgeable before release.

Platform: KnowBe4 - Uses KnowBe4 for phishing campaigns and training.

Tool: report phishing button - Uses the "report phishing button."

Background security assessments - Has tests and assessments on security and security policies in the background.

Effectiveness measure: click-through rates - Primarily measures effectiveness by click-through rates from simulations.

Opening email not indicator - Opening an email doesn't tell anything about engagement due to email client settings.

Main challenge: human element - The human element is the biggest challenge.

Challenge: non-technically proficient group - Has a huge group of people who are "excessively technically not great."

Challenge: fear of computers - Some employees have a "fear of computers."

Challenge: low baseline knowledge - Very low baseline IT knowledge level in many employees.

Challenge: language barrier - Language barrier is a challenge.

Consequence: high click rates (countries) - High click-through rates in certain countries due to lack of understanding.

Specific threat: C-suite spear phishing - CEO and C-suite get spear phished.

Motive: financial fraud - Main risk is financial fraud (invoices, getting them to pay something).

Financial control - Financial control (multiple approvals) is a different type of control.

Highest IT risk: password reset scams - Password reset scams using company name/user name are the highest IT risk.

Risk of being on hacker radar - Fear that people falling for scams could put the company on a hacker's radar.

Technical tools: exchange standard - Standard tools in Exchange.

Technical tools: scanning & blocking - Everything is scanned and blocked.

Lenient system - Only flagged items are moved to quarantine.

Technical vs. training as complementary - Sees spam filter/defender and training as complementary, not replacements.

Training success - Training will succeed in raising general awareness.

Training aim: conscious thinking - Hopes to make people more conscious and not immediately trust things.

Current training focus: email medium - Primarily focused on email as a medium.

Future threat focus: voice/video phishing - Future training will focus on video calling/phishing (vishing) and phone calls.

Reinforcement: repetition philosophy - Whole philosophy is repetition.

Reinforcement frequency - Aims for something at least every three months.

Personalization: both targeted & general - Wants to do both targeted and general simulated phish.

Targeted emails higher success - Targeted emails have much higher success rates.

Segmentation: by failure (additional training) - People who fall for phishing will get additional training.

Segmentation: country/language specific - May do country-specific or language-specific modules.

No role-based segmentation (IT knowledge gap) - No role-based segmentation because IT doesn't know employee roles.

Staying updated: online resources - Reads tech sites, security reports, newsletters.

Policy: contact IT for incident - Clear policy is to contact IT for incidents, password reset.

End-user gap: not reporting incident - End users might not report if they just close browser, or don't realize severity.

Communication need: user responsibility post-click - Communication needed on user responsibility if they suspect phishing.

Idea: big red button for incident - Suggests a "big red button" on IT page for easy incident reporting/priority.

No current barriers - No significant barriers at the moment.

C-suite support - C-suite actively supports training because they are actively phished.

Budget not prohibitive - Platform is not free, but not excessively expensive (~6 euros/person/month).

Managerial reception good - Managerial level reception is quite good.

Challenge: ensuring completion - Main challenge is ensuring all employees complete assigned training.

Engagement strategy: presentations/feedback - Hopes to do small presentations on numbers and get feedback.

Can't avoid "checkbox exercise" - Believes it's impossible to completely avoid training becoming a "checkbox exercise."

Past experience: monthly training is stupid - Mentions previous experience with banks, monthly training was "just stupid."

Training level: lowest common denominator - Training is made for lowest common denominator, level not high.

Training is "chore" for tech-savvy - For IT/knowledgeable, training is often a chore.

Engagement strategy: interaction required - Try to make training engaging with small videos, silly games, requiring interaction.

Current priority: monitor new training - For now, just want to keep doing current training and monitor results.

Platform content stagnation - Current platform (KnowBe4) not adding much new content, recycling older training.

Future platform consideration - Might need to move to other platforms for more gamified options.

Adaptive strategy - Will move on if current approach doesn't work, unless severe increase in danger.

Likely future format - Will likely stick to web-based small training, maybe presentations.