# Locked Out

| Domain | Policies and Procedures for Incident Response |
|---|---|
| Topic Covered | Procedures in Incident response |
| Learning Outcomes | • Acquire the basics of responding to a breach or attack<br>• Strengthened approach on reactions to incidents in the organisation<br>• Improved understanding of the appllicable techniques to mitigate damages and prevent further intrusion |
| Duration | 60 minutes |
| Kind of Method | • Presentation and group work<br>• Thinktank |
| Required Materials | • Projector<br>• Support Material for Host (Flowchart) |

Co-funded by the European Union

www.cyberyouthproject.com

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 the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them

2021-1-IT03-KA220-YOU-000028668

| | |
|---|---|
| Learning Setting and Activity Description | Preparation:<br>Complete Module 5 of the Cyberyouth course.<br><br>In class:<br>slides 1-2: the facilitator introduces the topic by explaining the main concepts around Incident Response and its importance in the global context of security<br><br>slide 3: Brief introduction to facilitate discussion, with the facilitator engaging with participants asking whether they have ever suffered an incident or breach and how they responded or resolved the situation.<br><br>slide 4: Explanation on some of the key points in incident response, the importance of having an established policy instead of improvising on the go.<br><br>slide 5-x: The facilitator proposes a ransomware situation and initiates a role-playing game where participants work as a group to formulate a response to the incident, with the facilitator playing the role of the attacker, indirectly guiding them to the correct response through reactions to the group's ideas. |

Co-funded by
the European Union

www.cyberyouthproject.com

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 the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them

2021-1-IT03-KA220-YOU-000028668

| | |
|---|---|
| Learning Setting and Activity Description | NOTE: This activity can be adapted to other types of attack if partners prefer. |
| Activity Evaluation/ Reflection | At the end of the activity, the facilitator will provide a PPT with discussion points such as highlights, dislikes and interesting points in the activity. |
| Supporting materials | Presentation: 🔗<br>Handouts: 🔗 |

Co-funded by the European Union

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 the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them

2021-1-IT03-KA220-YOU-000028668

# Fix the Flaw

| Domain | Policies and Procedures for Incident Response |
|---|---|
| Topic Covered | Procedures in Incident response |
| Learning Outcomes | • Acquire core knowledge on how to rebuild or improve security after an incident<br>• Improved understanding of ideal reocurrence prevention policies<br>• Greater skill in identifying the procedures to follow in re-securing an organisation's system after suffering an attack |
| Duration | 60 minutes |
| Kind of Method | • Presentation and group work |
| Required Materials | • Projector<br>• Whiteboard/Flipchart<br>• Writing Instruments |

Co-funded by
the European Union

www.cyberyouthproject.com

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 the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them

2021-1-IT03-KA220-YOU-000028668

| | |
|---|---|
| Learning Setting and Activity Description | Preparation:<br>Complete Module 5 of the Cyberyouth course.<br><br>In class:<br>slides 1-2: the facilitator discusses the importance of "fixing" the issues that caused a breach or incident to ensure this doesn't reoccur, along with how to identify and analyse the possible issues.<br><br>slide 3-5: Facilitator shows some common incidents and what can cause them, easy-to-make mistakes that have simple solutions, as well as destigmatizing making mistakes and emphasizing that in an incident, it is important to be honest instead of trying not to "look bad".<br><br>slide 6-x: Situation drills in which the facilitator demonstrates a hypothetical breach, while participants suggest what the probable cause was and how to resolve the flaw and how to prevent further incident. |

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 the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them

2021-1-IT03-KA220-YOU-000028668

| | |
|---|---|
| Learning Setting and Activity Description | |
| Activity Evaluation/ Reflection | At the end of the activity, the facilitator will provide a PPT with discussion points such as highlights, dislikes and interesting points in the activity. |
| Supporting materials | Presentation 🔗<br>Handouts: 🔗 |

Co-funded by the European Union

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 the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them

2021-1-IT03-KA220-YOU-000028668

# 4 Phase Detective

| Domain | Policies and Procedures for Incident Response |
|---|---|
| Topic Covered | Procedures in Incident response |
| Learning Outcomes | • Acquire the basics of incident forensics<br>• Strengthened approach on investigating and analysing information in a breach or attack<br>• Improved understanding of the importance of proper follow-up in ensuring no further damage is done |
| Duration | 60 minutes |
| Kind of Method | • Presentation and group work<br>• Thinktank |
| Required Materials | • Projector<br>• Flipchart<br>• Pen and paper for participants to take notes<br>• Reference sheet for facilitator |

Co-funded by the European Union

www.cyberyouthproject.com

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 the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them

2021-1-IT03-KA220-YOU-000028668

| | |
|---|---|
| Learning Setting and Activity Description | Preparation:<br>Complete Module 5 of the Cyberyouth course.<br>In class:<br>slides 1-2: the facilitator discusses digital forensics in the context of incident response (and also perhaps asks participants to explain their idea of digital forensics)<br>slide 3-8: Facilitator explains in layman's terms with a few analogies the meaning of digital forensics, as well as the 4 phases.<br>slide 8-12: Three hypothetical breaches are shown, whilst the facilitator divides the flipchart in to 4 sectors to represent the 4 phases of digital forensics. The participants will then take turns "investigating" by writing down information they consider pertinent in the appropriate sector, with discussion among participants as to whether it is correctly assigned or belongs in another sector. |

Co-funded by
the European Union

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 the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them

2021-1-IT03-KA220-YOU-000028668

| | |
|---|---|
| Learning Setting and Activity Description | |
| Activity Evaluation/ Reflection | At the end of the activity, the facilitator will provide a PPT with discussion points such as highlights, dislikes and interesting points in the activity. |
| Supporting materials | Presentation 🔗<br>Handouts: 🔗 |

Co-funded by
the European Union

www.cyberyouthproject.com

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 the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them

2021-1-IT03-KA220-YOU-000028668