SIEMENS
Ingenuity for life

Teachers Guide

Siemens Cybersecurity Challenge

The Siemens Cybersecurity Challenge aims to supplement Computing lessons at KS3.

The challenge is designed to familiarise students with cybersecurity to enhance their safety online and improve their knowledge and understanding of risks to their personal information online.

Students will also develop an understanding of security logs and how they can be used to spot fraudulent behaviour on a network.

Overview

Resource contents

+ Copies of the security log
+ Caesar Cipher Wheel template
+ Copies of suspicious emails
+ Copies of the location social media information
+ RFID materials
  - RFID template
  - Aluminium foil
  - Duct Tape
  - Scissors
  - Double sided tape
+ Mission Card to record all the findings

Learning outcomes

+ Understand how to identify common signs that can indicate fraudulent activity in a security log
+ Develop an understanding of why strong passwords are important and how to create them
+ Identify what to look out for to spot a phishing email
+ Learn how the information we post online can be used against us, and how to limit risks when using social media
+ Students will learn about the risks of Radio Frequency Identification, a system that uses radio waves to read, transmit, and capture information stored on a tag that is attached to an object

Suggested timing

+ 60 – 70 minutes

Siemens challenge introduction

+ **Suggested time: 10 minutes**
+ Introduce the topic by explaining that the class have been set a mission to help solve a problem centred on cybersecurity. Gauge the students' understanding of cybersecurity by asking the following prompt questions:
  - **What is cybersecurity?**
  - **What is an online cybersecurity breach?**
  - **What examples have you come across in the news about keeping safe online?**
  - **What kinds of steps do you personally take to be safe online?**
+ Use the board to write down all the things they say. Highlight a word they said that relates to network security or unauthorised access (they may have just said hacking)
+ Begin by discussing how cybersecurity is more than just sitting at a computer and writing code. Explain how cybersecurity is using technology to see the out of place and unusual things in data to find and catch cyber criminals.

1. Find the security breach

SIEMENS
Ingenuity for life

Instructions:

+ **Suggested time: 10 minutes**
+ Show a section of the security log (see below) and ask the students to identify the headings from the data. Delete the field names before showing to the students.
+ Once they have identified the field names hand out the full log and show the class the following scenario on the board:

Siemens suspect that a cyber criminal has been trying to log on to their system. You have been given a printed copy of a security log. This is a log that contains records of security-related events such as log-ins and log-outs. The security log is one of the main tools used to detect and investigate unauthorized activity (or attempts).

+ Tip: Add a competitive element to the task by splitting the class into teams of 4-5 students
+ Instruct the students to analyse the content to identify strange patterns in the data
+ Use the following prompt questions to support their data analysis:
  - **When did the breach happen?**
  - **What type of device did the cyber criminal use?**
  - **Which user was hacked to get access to the system?**

Extension task

Ask students to reason why they have got to that answer? The most suspicious log starts from 23/04/2019 at 22:58:58 from JK-SIE. The time, number of attempts, event info and device used are all unusual patterns.

DATE	TIME	USER	EVENT NAME	EVENT INFO	USER DEVICE
22/04/2019	07:45:23	ADMIN-SIE	SYSTEM STATUS	DIAGNOSTIC	FG-HP
22/04/2019	08:02:46	ADMIN-SIE	LOG OUT	SUCCESS	FG-HP

2. Confirming the culprit

Instructions:

+ **Suggested time: 10 – 15 minutes**
+ Next, show the class the following breakthrough that Siemens need their help with:

  Siemens has used the information you found about the cyber criminal to identify the device they used. The cyber criminal left a password protected PDF on the device and Siemens need your help to crack the password.

+ Gauge pupils' understanding about password encryption by leading a class discussion on the following questions:
  - **What is encryption?**
  - **How do you encrypt a file with a password?**
  - **When might you want to encrypt a file?**
  - **Why is encryption an important tool? What benefits does it provide?**
+ Explain that the Caesar Cipher is one of the simplest and most widely known encryption techniques. It is a substitution cipher, for example, with a left shift of 3, D would be replaced by A, E would become B, and so on. The method is named after Julius Caesar, who used it in his private correspondence. Give a short demo on how to use one of the ciphers
+ The PDF should be made available to the class via a VLE or shared drive. If you can't do this, have a hard copy of the contents ready to hand out when the students give you the correct password
+ The correct password is 'PNRFNECNFFJBEQ'
+ Support the students until they successfully open the PDF and get them to write down the criminal's identification (found in the payment details on the invoice)
+ Summarise by reminding students what makes a strong password that can be hard to crack. A strong password:
  - **Has 12 characters minimum**
  - **Includes numbers, symbols, capital and lower-case letters**
  - **Isn't a dictionary word. Avoid obvious dictionary words or any others related to you e.g. where you live**

Extension Task

Students could code their own messages or add in new rules to the cipher to make it stronger. For example, using a numerical pattern or adding numbers to vowels.

3. Secure the evidence

Instructions:

+ **Suggested time: 10 minutes**
+ Ask the class if they know what phishing is and have they or anyone they know, experienced it before?
+ Use the board to record their thoughts and guide their answers to identify that phishing is an email disguised to look more trustworthy, for example using branding from a well-known company. Phishing emails normally are trying to steal login credentials, personal information or credit/debit card numbers
+ Explain that the next task is to look at some email examples and identify whether they are phishing emails
+ Hand out the emails to the students and give them three minutes to look through them
+ After three minutes, write the answers on the board. Students should note these answers on their mission cards

4. Find the criminal's location

SIEMENS
Ingenuity for life

Instructions:

+ **Suggested time: 10 minutes**
+ Students should have completed their mission cards up to this stage
+ Explain to students that what they post online can contain information we might not necessarily want everyone to know. This can include street names and unique things like a view from a bedroom onto a landmark
+ Hand out the mood boards and explain that they are looking for clues about the location of the cyber criminal
+ Support students to look through the clues and note down anything they think could help identify where the cyber criminal might be. Encourage students to look out for landmarks, street signs in photos and location tagging in posts:
  - **The correct location is 42 Devonshire Terrace, London, UK**
  - **The house number is shown in the café post**
  - **The street name is Devonshire Terrace**
  - **The town is identified by the well known locations and post captions.**

5. Get ready to go out in the field

Instructions:

+ **Suggested time: 15 – 20 minutes**
+ Congratulate the class on passing their 'cyber agent training', they are now ready to 'go out into the field'
+ Explain that as cyber agents they will get an ID badge. You may have a security badge for your school or one for the photocopiers, this may work on RFID. This technology is increasingly widespread, particularly for contactless payments, but also for key cards and passport chips. Criminals with can construct their own RFID readers with cheap, minimal supplies. These devices can steal private financial information without the victim knowing
+ Ask the class in pairs to identify some of the dangers of losing personal information to a cyber criminal
+ Explain that to keep our information safe they are going to create RFID blockers. Explain that these do not stop the RFID from working completely, but do prevent the card from transmitting as far, so a card reader would have to be much closer to the card
  - **Support students to cut out the card sleeve template**
  - **Cover the inside of the card sleeve with aluminium foil and duct tape it securely in place**
  - **Students should tape over the entire surface of the foil to prevent it from tearing during use**
  - **Use a pair of scissors to scour the folding edges of the sleeve on the inside**
  - **Fold the sleeve and secure using double sided tape on the inside of the flaps**

Advancing cybersecurity – The Charter of Trust

Currently, Siemens has approximately 1,275 cybersecurity experts worldwide, which includes 25 white-hat hackers who continuously challenge the security of both internal IT systems and products being shipped to customers.

In 2018, Siemens and eight industry partners signed the first charter for greater cybersecurity. Initiated by Siemens, the Charter of Trust calls for binding rules and standards to build trust in cybersecurity and further advance digitalisation.

The charter encompasses 10 key principles which have been identified by the signing partners as essential for establishing a new charter of trust between society, politics, business, and customers. The sixth principle is Education, and this highlights the commitment of Siemens and partners to lead the transformation of skills and job profiles needed for the future.

For more information, resources and activities visit: siemens.co.uk/education