HackShield Lesson Manual

Class Quest 5 - Phishing

Lesson duration

45 minutes

Target group

Suitable for students between the ages of 8 and 12.

Learning

Students learn...

- what phishing is.
- how to recognize phishing.
- what to do when dealing with phishing.

Necessities

- Interactive board
- Teacher account for HackShield (create it here)

Concepts*:

Personal data: data which can be directly traced back to you as a person. Think of your name, address or place of residence, but also your telephone number, zip code or names of your family or pets.

Phishing (message): Phishing is a form of online stealing, and as such a cyber crime. Phishing is when a criminal sends you a message to retrieve login details, bank details or other personal information. “Phishing” comes from the English word “Fishing”. In this case, criminals are fishing for your online personal information. *Fun fact:* In the 1980s, many hackers used the “ph” instead of an “f”. So “Fishing” became “Phishing”.

** Would you like to know more about the above topics? Go to joinhackshield.com and watch the videos for inspiration and in-depth knowledge. Then you are fully prepared for this class!*

General

In this class quest students will find out what phishing is and how they can recognize it. For example, criminals impersonating your bank, school, or insurance company and asking for personal information. You can also receive an email stating that you have won a big prize or receive a WhatsApp message which says you will receive a large inheritance from your grandmother. In this class, students are given tools from which they learn to look critically at their messages. For example, there are often small errors in the message, such as spelling errors or an error in the URL such as .ccom instead of .com.

The Phishing Lynx, explains the tricks hackers use to trick you into something. This way you don't fall for it!

Good to know

Take a look at the website HackShield so you can see what the game environment and the class quest look like, so you know what your students can expect. This takes about thirty minutes.. Don't forget you need a teacher account for this, which you can create here.

Elaboration

Introduction - 10 min

Explain to the students you are going to talk about the term Phishing, what it is exactly, and you will play a game about it together.

Together with everyone on the internet, we spend so much time online! More and more communication is done online and we also share a lot of links (URLs), images and other messages with each other. Accidents happen easily. How often does it actually happen that you just click on something without checking if it is safe? Just because you already click, type, swipe and scroll so much.

Introduction questions

- How often do you click on a link without thinking about the security of it? Does this ever happen?
- What did you do when this happened?
- Can we think of situations together where you might click on something? *(for example: you are in a hurry, you want to send something quickly or you have cold fingers.*)

Optional

Students make a phishing message in groups (or simply draw/write it on a piece of paper). Students can take this home and show it as an example at home so they never have to fall for it again!

Core - 30 min

Start the quest on the interactive board. Inform the class you are now going to start the game and discuss rules that suit your class when you play a game on the interactive board as a class.

Tips

- Do you want to mute the sound in the quest? You can do this in the game's menu through the gear wheel. Move all sliders to the left (Music, SFX & Video).
- In the quest, the Phishing Lynx and André tell you all about phishing. This is described in text. You can decide to have children read the text of a specific character (for example, child x reads André's text and child y reads the Lynx's text). The individual messages that appear on the screen can always be read by another student.
- During the quest, certain choices will have to be made. You can choose to use an active work form. For example: If you think we should go right, you can stand. If you think we should go left, you can sit on the floor.

Class activities in the quest

The questions below are shown as class activities in the purple Queries (it looks like a robot) in the quest. As a teacher you can decide whether you want to do the activities. We recommend discussing these questions with your class to promote awareness of the online choices they can make. Of course you can choose to skip this or discuss it at another time.

- **Have you or someone close to you ever received a phishing message? What did you do then?**

- **Can you also receive phishing by mail?**
  Yes, you can! For example, fake letters from the bank.

Closing - 5 min

Ask the students what they have learned.

Final questions

- **How do you recognize phishing?**
  Possible answers:
  - *You can recognize unusual things by reading carefully.*
  - *Keep an eye out for spelling mistakes.*
  - *Phishing messages often start impersonally.*
  - *You often have to do something "FAST".*
  - *You often have to click on something or download something.*
  - *There are suspicious sentences in it.*
  - *It's an unusual e-mail address or an e-mail address with spelling errors.*
  - *Companies NEVER use @hotmail.com, @gmail.com, @outlook.com or @msn.com*
  - *Link shorteners are used such as T.co, bit.ly and Goo.gl.*
  - *It says: "Click here to login" - Never do this. Hackers copy websites. Go to the correct URL yourself and log in.*
  - *There are strange words in the links.*
  - *Do they speak, or use, a different language?*
  - *By a foreign phone number being used.*

- **There are a number of suspicious phrases that hackers often use. Which one do you know?**
  Possible answers:
  - *We are working on a security update, check your details*
  - *I work at the bank, can I check your details?*
  - *You have won a prize*
  - *Your account has been blocked*
  - *The settings for your internet banking are not correct*
  - *You receive an inheritance from an uncle you do not know*
  - *Transfer money and earn even more money*
  - *Forward this message to as many people as possible*
  - *The postman has tried to parcel to be delivered, but no one was home*

Shield & Points

When you complete the quest with the students, you will receive a code at the end. When students have created their own profile on joinhackshield.com (look at the appendix to know how you could guide them in this), they can fill in this code, which earns a shield and extra points.

Tips

- Write the code on the board or have students write the code themselves to take home. In this way, you encourage students to delve further into cyber security at home. What else do you want!?
- Do you want your students to play HackShield more in the classroom? That is of course also possible. The appendix explains step by step how you can guide the children to create an account.

Appendix

How to create a HackShield account with the students

The students can continue their cyber path in HackShield at home or at school, but they need their own account for that. By encouraging them to come up with a suitable username and password, you help them make safe choices online. Below are some tips:

(Do you only want to know how to create an account on joinhackshield.com? Then only read the bold text at point 4)

1. Take the password crack test as a class. Have students count the number of characters in their most commonly used password. So also ask whether it contains capital letters or numbers, for example. Enter a password on the website and you will see how many years or sometimes even seconds it takes to crack a password.
2. State that a passphrase is a good and safe option. Such a sentence does not have to be difficult. As in a written sentence, have them also use the spaces between the words as characters. Bet that a hacker can crack that difficulty? Hackers, as well as automated password crackers, have a hard time trying to figure out many consecutive characters. Just count the characters of a passphrase and fill it in on a password cracking test. Do you see the difference?
3. Hackers always check what they can already find about you online. So never use your name or date of birth in your username or passphrase!
4. **Show the students that they can click LOGIN/REGISTER at the top right of joinhackshield.nl. Then they have to click on the big blue REGISTER button and they can fill in all their details there. Have they created an account? Then they can click on the big orange PLAY button at the top right of the website.**
5. Before everyone gets started, you go through the first steps together. The game speaks for itself. Mention that this game is not about speed, but about answering most questions RIGHT. It contains tips and new insights that can come in handy to prevent hacking.
6. There are a lot of difficult words in it. Students can of course always Google them! It is useful if they write it down immediately, so that you can discuss a number of those concepts with each other at the end of the lesson (power of repetition).