# Hacker Highschool

## SECURITY AWARENESS FOR TEENS

# CONTRIBUTOR'S GUIDE
# CREATING GREAT LESSONS

WWW.ISECOM.ORG / WWW.OSSTMM.ORG / WWW.ISESTORM,ORG / WWW.HACKERHIGHSCHOOL.ORG

# “License for Use” Information

The following lessons and workbooks are open and publicly available under the following terms and conditions of ISECOM:

All works in the Hacker Highschool project are provided for non-commercial use with elementary school students, junior high school students, and high school students whether in a public institution, private institution, or as a part of home-schooling. These materials may not be reproduced for sale in any form. The provision of any class, course, training, or camp with these materials for which a fee is charged is expressly forbidden without a license including college classes, university classes, trade-school classes, summer or computer camps, and similar. To purchase a license, visit the LICENSE section of the Hacker Highschool web page at www.hackerhighschool.org/license.

The HHS Project is a learning tool and as with any learning tool, the instruction is the influence of the instructor and not the tool. ISECOM cannot accept responsibility for how any information herein is applied or abused.

The HHS Project is an open community effort and if you find value in this project, we do ask you support us through the purchase of a license, a donation, or sponsorship.

All works protected under Creative Commons 3.0 Attribution-NonCommercial-NoDerivs 2001-2010, ISECOM.

# Table of Contents

## Contributors

*Those who create and contribute to these lessons are listed prominently in each lesson. Your name will go here for helping make this project the best it can be!*

Contributor, Place of Work, Contact Info

Pete Herzog, ISECOM, pete@isecom.org

# 1.0 Introduction

So you want to write lessons for Hacker Highschool? We think that's great! But to be truly helpful you need to understand a little bit deeper about this program.

Firstly, these lessons are written to teenagers. In order to do that, we did our research on how we do exactly that. Which is why from the title, the theme, and the goal, this project will seem to many adults that we're playing with fire. They think we are giving the keys to some powerful knowledge to kids. Perhaps this is seen as a gateway to future criminal activity. But anyone who has worked with teens, who have tried to reach them, engage them, and get them ready for their future are very aware that this is just not true. Teens are young adults who are guided by specific needs as part of growing up. So as part of the ISECOM Smarter Safer Better project (www.smartersaferbetter.org) we have applied here what we know through scientific psychology, neurobiology, and sociological research about how teens learn, act, socialize, believe, and behave. And that's what you need to know too to write these lessons and promote HHS properly in schools.

What do we know about these “kids” who are old enough and developed enough to procreate yet not vote or possibly even drive? We know they can get deeply interested in certain topics if it challenges them but they are quick to give up on things before they try them (just in case they fail while trying). We know their amygdala is still forming which gives them poor working memory and poor risk decision skills. We know they don't project themselves as easily or as much as adults meaning they are not likely to think they can do something that they see someone else do. So they will surprise themselves if they try it and can do it. We know that they value short-term rewards over long term. We know where they are given the chance to do something that has great reward despite great punishment they will prefer to take the chance to get the reward. We know that they can learn to make logical, rational, “right” decisions but will forget all that proportionally to how emotionally (or hormonally) involved they get in it. We know that they will remember and hold onto knowledge they figured out for themselves more than if they are told it, except if it's form a friend they respect.

What does this mean to Hacker Highschool? It means that our lessons must be engaging, progressively challenging, but easy to do. We need to make the lessons open with hints on where they can get the answers. We have to be sure that every question they answer can lead them to discovering similar or deeper knowledge if this particular thing piques their interest. We need to make sure that they learn for themselves and come to solutions on their own. No spoon feeding! We need to push the reward and thrill of discovery and the power of knowing deeper knowledge of how something works yet constantly show them there is always more to know. That will get them to respect their limitations and still encourage them to stay up to the challenge of defending themselves.

So in this program, the first thing teens learn is that they can get easily hacked. They had no idea they were so exposed. So they get interested and start to naturally respect the concept of hacking and they have the confidence to try defending their systems and devices. As they get better and their training continues, they realize that there is so much to do and learn still that even if they could break into a system, there's no way they can do it and not get caught by the people who are much more advanced than they are. Eventually, as they improve and reach the point where they learn how to mostly evade capture, they realize they can really hurt someone if they wanted to now. And knowing that gives them enough self confidence and self satisfaction that it restrains them even more from using their skills in an offensive way.

So as a creator or reviewer of these lessons, you need to focus on delivering those three things to the teens taking these lessons: respect, self confidence, and realization.

We want to encourage students to be creative, resourceful, and critical thinkers. The core instruction theme is to harness the hacker curiosity while applying critical thinking skills and guide the students progressively through their hacker education. The goal is to help them grow into a responsible role, capable of determining security and privacy problems, and making proper security decisions for themselves.

Your role in this is to guide them into learning what they need to know about a security or safety topic by engaging their curiosity and their love of problem-solving. To help them learn something on their own rather than spoon-feeding them the answer is not only much more rewarding for them but also greatly increases their retention of the lesson.

This Contributor Guide will show you how to structure your new HHS lesson, how to add the right content which will engage the young hacker, and explain how to provide consequences within the lesson so that they have a clear understanding of what happens and who is impacted by any random hacking they may be considering outside the scope of the lesson, something we don't want to discourage completely but do want it within the framework of responsible hacking.

## 1.1 Getting Started

How do you write lessons to reach hackers or those who want to be hackers? We start with a topic. You can pick anything that's new or old which is relevant in their lives but what's most important is that it's there to challenge them to get want to understand it and that it will inspire them to keep going.  For an example to use as we go along in this guide, let's use the topic “*Firewalls*”.

After you have a topic you need to explain to them what it does. This does not mean you need to make an encyclopedia entry. You want to give them ideas about the topic from the viewpoint of how a hacker should see it. This will show them how to see things operationally and critically. You should feel free to use professional terminology and when you do so, underline those words. For example:

> *The primary gateway defense for most networks is the firewall, a server that routes packets to the destination and back out again, while rejecting and dropping connections that don't match its rule base. The firewall rules can be built on any information that's in most any kind of packet including the data but at the very least, those delivered over TCP, UDP, and ICMP. Firewall rules can even filter on time, date, frequency, fragmentation, and order of connections. Which means that the firewall has to see what's in the packet to stop it. This is what makes encrypted sessions over HTTPS, SSH, VPN, and other confidential protocols so interesting because the firewall usually can't read the data that's in an encrypted packet because that's only between the server and the client. Sure it's possible that the firewall initiates and terminates the encryption but there are often ways to find out if that is indeed what is happening. So the firewall can't stop what it can't read.*

Writing like this gains the interest of the curious reader and encourages them to read up on what they don't know. So it is important to not explain too much of the vocabulary and instead focus on what you can do with it. This is the essence of the self-learning lesson. If you want to make resourceful people, you need to start with lessons that force them to be resourceful.

You will also want to stick with a particular lexicon. We use the glossary from the OSSTMM 3 so it is important you are aware of how operational security is described accordingly. However, this is not as important as writing a captivating lesson. So do your best and let ISECOM fix things like that in the final edits.

### 1.1.1 Structure

You can build your lesson based on the following structure:

1. Introduction to what this lesson covers
2. Getting Started, what materials you need and what the goals are of the lesson.
3. How the topic works from a hacker's perspective which is a mix of an analysis of how people use it, how it should work, and how to see if it can be made to work in other ways possibly not intended by the maker – this can take up multiple pages and be multiple sub topics. Don't feel the need to explain too much but don't be afraid to explain interesting or little known facts either. Most importantly, stick to the facts. Don't put anything into the lesson that gives generic advice, focuses on best practices, or makes illogical claims. Which brings us to our last bit of advice- apply logic where possible. It gives the hacker a chance to see discriminating advice in action and therefore it creates something positive that the reader can repeat and reapply in other areas of life. For example:

> When specific tools have been used by the vendor to test a firewall to show how impenetrable it is, look at the tools. Ask yourself: How were they made? Why were they made? Do you think tools can be made smarter than the people who make them? Can tools give results smarter than the people who can understand them? So any firewall tested with a tool is at the limit of both the tool and the analysis of the results. As a hacker, your goal is to push both.

4. Create exercises and small quizzes to keep the hacker engaged. You can make these a part of the topic lesson or put them at the end of the lesson. However smaller exercises more often will get more attention and be easier to manage than a large one at the end.
5. Resources and further reading, this will keep the reader going and growing!

## 1.1.2 Challenging the Hacker

The use of short answer type exercises is a great way to engage the reader in a way that can allow their creativity to flow and feel good about their learning progress. You will need to create questions pertaining to the lesson that pique their curiosity, make them think through multiple steps for a conclusion, and require them to be resourceful. That means the answers are not in the text of the lesson and not necessarily somewhere they can find on a web page but rather something they can deduce or determine on their own. Most of the work of such lessons is creating the right exercises that will challenge yet still be possible to solve. A good template for a good question is one that if you asked a professional their likely answer would be “it depends”. Questions like that will encourage the readers to keep trying to frame the question as they follow multiple paths and trials to determine the answer. So do stay away from canned answers which mistakenly enforce 2 myths in hacking: there is only 1 way to do something and what you get now you will always get.

Some sample exercises for our firewall sample lesson may look like the following:

### 1.1.2.1 Exercises

1. What kind of firewall rules on your own network would effect how you run a port scanner through it to test a server somewhere on the Internet?

2. Explain what might be happening if you send a TCP SYN packet to a web server but you get no reply and you know the web server is there because you can see the web page?

3. How would you use a firewall to protect a web application on a web server from hackers? ***(Using nearly impossible to answer questions is a good way to introduce them to the puzzle of security and how there may be no “right” answer. It shows them there is always more they need to learn.)***

## 1.1.3 Formatting for Delivery

In the format, the X.Y.Z outline structure allows us to keep the lessons growing. The X is for the lesson number, the Y is for the main category, and the Z is the sub category.

It is recommended you stay with this structure for writing the lessons. Feel free to use a copy of this lesson and the format to build your new lesson. This structure allows readers to compare notes with other readers, build upon previous lessons, and keep notes on their progress.

## 1.2.0 Last Remarks

Remember that you are trying to engage young, clever, and curious minds that have poor risk analysis skills. Feel free to teach things that might be "dangerous" however do let them know about consequences for straying outside the HHS test network in such cases. The reader is ultimately responsible for their own behavior but you are responsible for making sure they know WHY something happens and HOW it can go wrong. Most of all, have fun writing your lesson because that will also make it fun for the reader to read it!