We use software all the time. From the smartphone alarm that rings when it’s time to wake up, to the application that allows us to video chat with friends and family that live far away, software is an important part of our daily lives.

How do you become an application security superhero? What do you need to learn?

Let’s start by learning the AppSec ABC’s!
AppSec is the practice of finding, fixing, and preventing security issues to protect a software application.
A data breach happens when private information is stolen by someone who is not supposed to have it.
Code is the language that people use to tell software applications what to do.
DevOps is a way to build software applications where teams work together to finish projects quickly.
E is for Ethical Hacking

An ethical hacker tries to break into a software application and then fix it, so that someone else can’t break into it the same way.
Sometimes security professionals use tools to help them find security problems in software. When those tools find a problem that turns out not to be a problem after all, it’s called a false positive.
To do application security right, someone has to think about the rules.

G

is for Governance
H is for Honeypot

A honeypot is used to distract a bad person from finding the real treasure.
When someone breaks into a software application, the team protecting that application steps in to try and stop the attack.
JavaScript is a computer language that can be used to program special things like flying robots!
K

is for Key Management

Just like it’s important to protect the keys to your house, it’s important to protect the keys that control access to digital information.
Logging is when you keep track of what’s happening. Computer logs can keep track of different things, like who tries to access what. This is similar to how a classroom attendance log keeps track of which students are present each day.
There are good software apps that you want to have, and bad software apps that you don’t want to have.

The bad software is called malware.
is for Null

When you count numbers, you count 1, 2, 3. When software counts things, it starts with null. Null, one, two, three.
Santa makes a list, and he checks it twice. OWASP makes a list of the most common ways for people to attack software. This is called the OWASP Top 10.
Pen testing is when a team of security experts hacks an application to find problems so that they can be fixed before bad people attack the software.
When a company (buyer) wants to buy software from a vendor (seller), the buyer will ask the seller questions about their security program. This is called a vendor security questionnaire.
R is for Red Team

A Red Team is a group of security experts that tries to hack into a system with a specific goal.
SQL Injection is a type of software attack where a hacker asks a computer database to do something it is not supposed to do.
A Threat is anything that has the potential to cause serious harm to an application. In the story of the Three Little Pigs, the threat is the wolf.
When someone goes to a place where they are not supposed to be, it’s called unauthorized access.
A vulnerability is a weakness. In the story of the Three Little Pigs, the vulnerabilities were the houses made of straw and sticks. These were vulnerable to attack by the threat, the Big Bad Wolf.
A whitelist is a list of things that are allowed.
XSS (Cross-Site Scripting) is a type of vulnerability that allows an attacker to change the information that is viewed in a user’s web browser.
It’s important to keep Your Personal Data safe. Protect your data and be your own application security super hero!
A Zero Day Vulnerability is a security problem that doesn’t have a solution yet.
Now that you’ve learned the AppSec ABC’s, you’re on your way to becoming a security superhero!