



Developer Security Toolkit

Empowering Teams to Deliver More Secure Software

Software developers, whether programmers, testers, designers or product managers, typically make hundreds of decisions every day. Very few of those decisions have security implications. It is vital that developers spot security-relevant decisions as they are encountered, and have a clear sense of when security is needed for different kinds of development tasks.

Based on our research, the Motivating Jenny project has designed a toolkit to help **sensitise** development teams toward security issues in the workplace. Each package has simple and complete instructions for you to use.

How does the toolkit work?

Developers like to solve problems. When they identify a security problem in their environment, most developers will actively try to solve it, whether by drawing attention to a security impact in a product management meeting, by using secure functions and constructs while coding, by thinking up tests of security, or by consulting an expert. It is vital to help team members develop their sense of when security activity is needed and why: to **sensitise** them to security.

Development teams and departments improve practice when they work together. The four packages in this toolkit, highlighted on the next sheet, were designed to complement other kinds of technical security training, offering you a simple way to help developers and teams to bring security to the forefront of team discussions and practice.



Security in the World

What:

A card-based workshop in which participants explore the impact of real-world security issues on developers and teams

Why:

It is not easy to contemplate how weaknesses in a product or service may lead to a compromise or breach. This workshop creates a safe space for participants to explore the consequences of cyber security attacks for companies and individuals.

When:

Lunchtime, Induction, Away days



Security in the Community

What:

A how-to guide that helps developers bolster their security know-how online

Why:

Learning security is about more than exercises and check-lists. It is about getting involved - engaging with real problems, and giving and receiving support from other developers.

When:

Spare moments, 10% time



Security and Me

What:

A self-assessment tool that prompts reflection and discussion about individual attitudes toward security.

Why:

Security is not only technical, it touches on who developers are and what they think is important in their work. This inventory helps developers explore their sense of why security is important.

When:

Between releases, Away days



Security Between Us

What:

A modelling workshop in which pairs examine active security issues in their teams.

Why:

Developers need the right conditions to make code secure. Teams can use this workshop to identify security practices that work well in their environment, and to point out areas that can be improved.

When:

Onboarding, Retrospectives