Welcome to the

CyberWayFinder

FOUNDATION OF SECURITY

2025

CWF
CYBERWAYFINDER

The CWF Foundation of Security is organized by CyberWayFinder and was first launched in 2017. Since then, it has been taken by more than 150 course participants. To find out more about their experiences read our blog or listen to the CWF podcast:

https://www.cyberwayfinder.com/podcast

CyberWayFinder Global
www.cyberwayfinder.com

This starter kit and all the information contained herein is intended for registered participants of the CWF Foundation of Security 2025 Cohort.

TABLE OF CONTENT

1. PROLOGUE

This is the tenth iteration of the CWF Foundation of Security since the program started offering career transition training tracks in 2017. The idea of a foundational course in cybersecurity is two-fold: one, to give a comprehensive high-level overview of the different domains of cybersecurity as it is practiced in large and small enterprises; and two, to introduce the course participants to foundational concepts, use-cases, and business and technical vocabulary used in the wide field of cybersecurity.

We are aware that it is an impossible task to understand everything there is to know in the Cybersecurity Common Body of Knowledge (CBK) in 14 weeks - so as an important reminder to all the participants: ***these weeks of intense learning will require some hours of self-study each week to go deeper into each topic of each domain***.

References and recommended reading materials will be regularly shared by the CWF team.

2. THE WIDE WORLD OF CYBERSECURITY

Cybersecurity is a very broad field.

In the media, it is often portrayed as a hacker's profession - but that is certainly a very narrow view of how cybersecurity is practiced as a profession.

The reality is that information technologies have reached such a level of complexity - there is too much diverse knowledge, experience and information required to be able to defend against any advanced persistent threat or respond to any cyber incident coming from cybercriminals and nation-state actors effectively.

CWF's mission is to build **a pipeline of talent from other professional fields** and help them pivot into the cybersecurity field, bringing new perspectives and skill sets into the field. The first step for any professional wanting to transition into security is to get a comprehensive view of the scope of security, how it is practiced in organizations, and to understand the different domains and how they overlap and relate to each other. Security is much more than just knowing how to hack into systems.

The main objective of this course is to give you the foundational knowledge of each domain of the **Common Body of Knowledge (CBK)** needed to kick-start a career in cybersecurity.

But cybersecurity is also about culture, vocabulary and sociology. As we progress through the program with you there will be many opportunities to explore and elaborate for yourself different areas.

Please engage with a **Beginner's Mindset** with the coursework, your cohort colleagues, the seminar facilitators, but most importantly with the greater cybersecurity community and conversations happening around the cyber world.

Become more comfortable and conversant with your **'Cyber Why'** and the domains and topics that interest you most.

3. COURSE WORK & MODULES

The Foundation of Security is based on the seven domains of the SSCP certification of (ISC)2 which is an entry-level cybersecurity administrator certification and is an ideal starting point for pivoting into security.

There will be weekly coursework of 3-4 hours - on-demand recorded coursework and virtual seminars - supplemented by 1-2 hours of reading assignment.

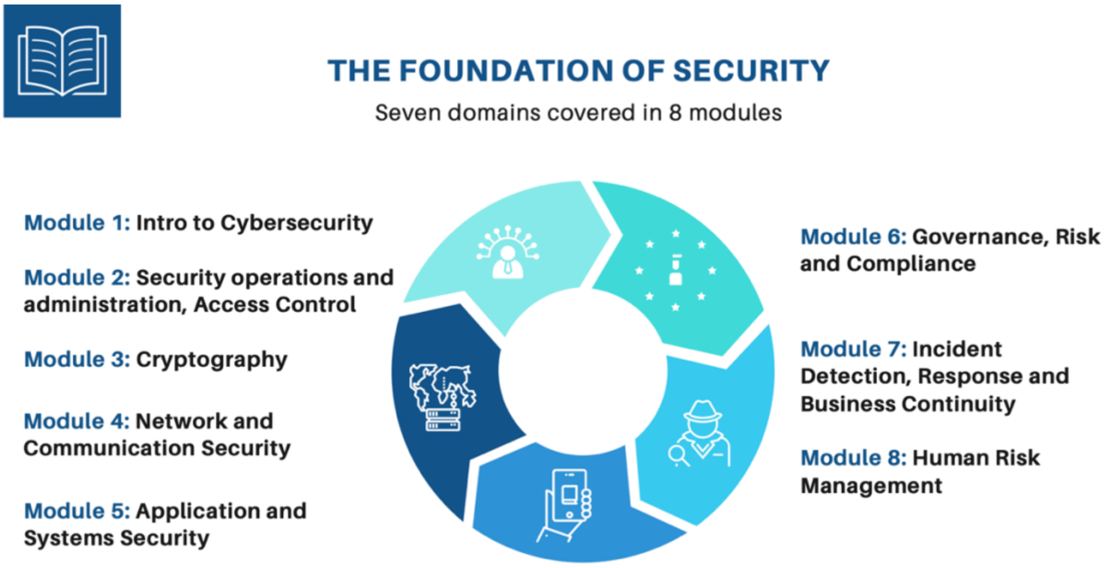
On-demand recorded coursework will be available on the CWF Learning Management Platform hosted on Odoo, where reading assignments, notes and references will also be shared. New content will be published every week.

Virtual seminars (live online) will take place on Saturdays 9:30-12:00. The seminars, as well as the kick-start session on 27 September, will take place in Zoom and will be recorded and shared on the learning platform.

These seminars will cover case studies and discussions on the topic of the week (see next section with weekly schedule of topics) and will be interactive.

For these online sessions, **we will require everyone to turn on their cameras and microphones**. The Zoom link to the virtual seminars will also be shared on the learning platform.

The Modules will be covering the following topics:



THE FOUNDATION OF SECURITY

Seven domains covered in 8 modules

Module 1: Intro to Cybersecurity

Module 2: Security operations and administration, Access Control

Module 3: Cryptography

Module 4: Network and Communication Security

Module 5: Application and Systems Security

Module 6: Governance, Risk and Compliance

Module 7: Incident Detection, Response and Business Continuity

Module 8: Human Risk Management

Suggested reference for this course is the (ISC)2 SSCP Common Body of Knowledge, or CBK (we recommend the latest eBook version – from Kindle or Google Books).

While not an absolute requirement, the coursework is roughly based upon the seven domains of the SSCP Common Body of Knowledge, and this book provides a solid and authoritative reference source for the program.

It will also be useful to place on your desk or on the bookshelf visible on your remote video conference setup as a signifier to everyone of your interest in, and academic pursuit of, professional cybersecurity matters.

5th Edition

SSCP.

Systems Security Certified Practitioner

An (ISC)^2 Certification

The Official (ISC)^2 SSCP CBK® Reference

Mike Wills

SYBEX A Wiley Brand

Furthermore, we sincerely encourage you to pursue and pass the SSCP exam after having completed the program as this is an important career milestone and credential (via a timed and proctored exam) that is internationally recognized by hiring managers, Human Resources professionals, and peers alike.

4. COURSE SCHEDULE

Date	Schedule: Foundation of Security SEPT 2025 - January 2026 (all time slots in CET)
Orientation Seminar 27.09.2025 Week 1 27.09.2025 - 04.10.2025	Introduction to the Course CWF Learning Platform, the Signal chat group and Code of Conduct, Interactive Introductions of the CWF team and the Cohort participants Sat. 27/09, 9:30-11:30 Module 1: Introduction to Cybersecurity Virtual Seminar: Sat. 04/10, 9:30-11:30
Week 2 & 3: 05.10.2025 - 18.10.2025	Module 2: Security Operation and Administration, Access Control Virtual Seminar 1: Sat. 11/10, 9:30-11:30 Virtual Seminar 2: Sat. 18/10, 9:30-11:30
Week 4: 19.10.2025 - 25.10.2025	Module 3: Cryptography Virtual Seminar: Sat. 25/10, 9:30-11:30
Week 5 & 6: 26.10.2025 - 15.11.2025	Module 4: Network and Communication Security Virtual Seminar 1: Sat. 08/11, 9:30-11:30 Virtual Seminar 2: Sat. 15/11, 9:30-11:30
Week 7: 16.11.2025 - 22.11.2025	Module 5: Application and Systems Security Virtual Seminar: Sat. 22/11, 9:30-11:30
Week 8 & 9: 23.11.2025 - 20.12.2025	Module 6: Governance, Risk and Compliance Virtual Seminar 1: Sat. 06/12, 9:30-11:30 Virtual Seminar 2: Sat. 13/12, 9:30-11:30
Week 10: 07.01.2026 - 17.01.2026	Module 7: Incident Response, Business Continuity, Cyber Resilience Virtual Seminar: Sat. 17/01, 9:30-11:30
Week 11: 18.01.2026 - 24.01.2026	Module 8: Human Risk Management Virtual Seminar: Sat. 24/01, 9:30-11:30
Week 12: 31.01.2026	Final Assessment: Virtual Seminar 1: Sat. 31/01, 9:30-11:30

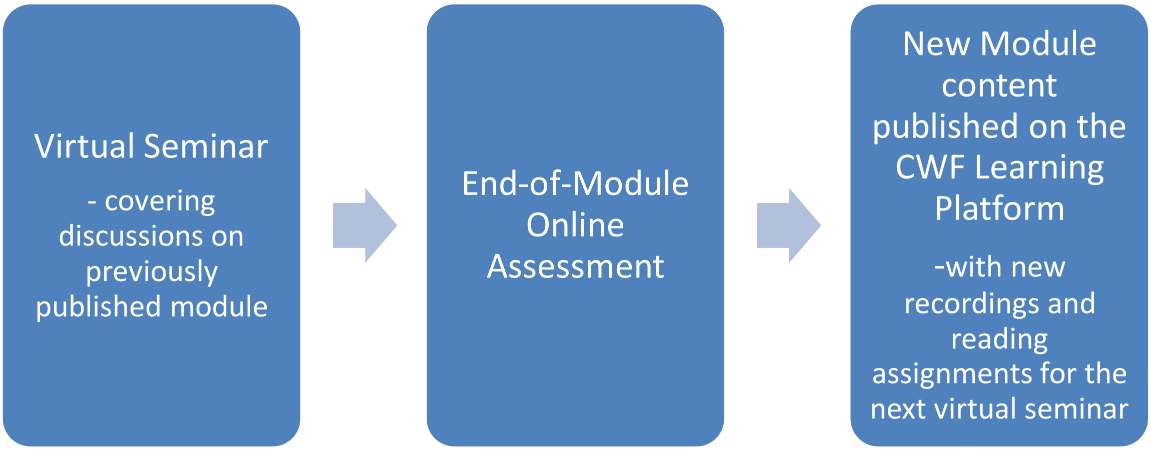
Each week (on Saturdays) new content - on-demand recorded course work, handouts or notes, and reading assignments - will be made available in the CWF Learning Management Platform, following the end of the live seminar of the previous week's topic.

Each module will end with a test assessment shared after the end of the last virtual seminar of the module. This will be completed online and will cover the content of the whole module.

The purpose of these tests is to assess your understanding of the delivered content of the past weeks' module. This is good feedback for the trainers and for the CWF team so they could help you better with parts of the material you need more support in.

We encourage you to actively participate in the virtual seminars and contribute through questions, sharing your own experience or your own perspective.

Actively interacting with new concepts and vocabulary, and repetition, help for long-term retention.



Virtual Seminar

- covering discussions on previously published module

End-of-Module Online Assessment

New Module content published on the CWF Learning Platform

-with new recordings and reading assignments for the next virtual seminar

5. COHORT CHAT GROUP ON SIGNAL

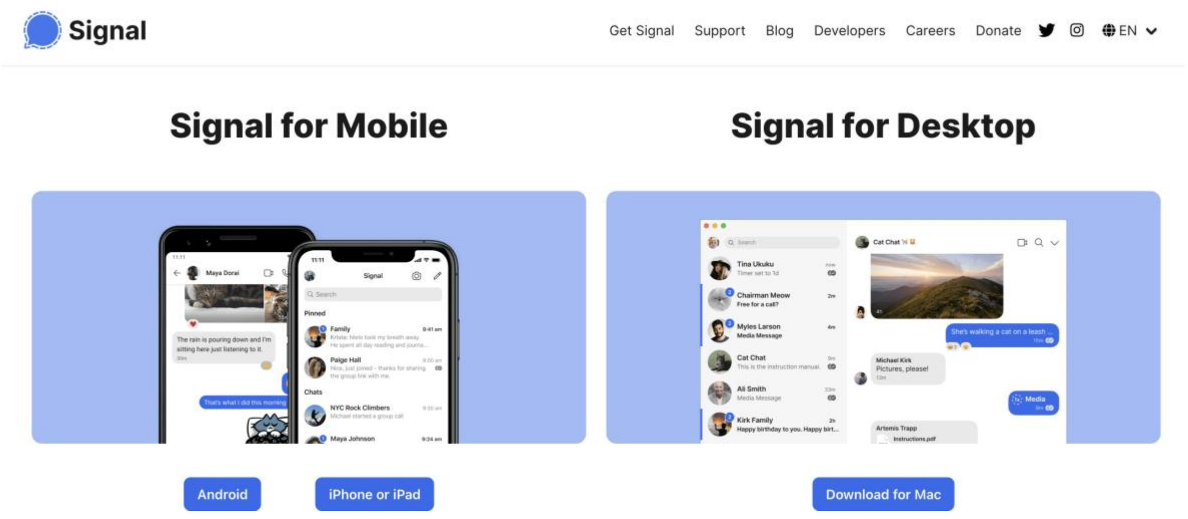
One of the best ways to learn is from each other!

Cohort-based learning increases the learning momentum significantly – so for each CWF cohort (this is what we call the group of participants following the FoS course at the same time) we create a chat group in the Signal messaging app, to stay in contact with the other course participants and the CWF team.

In the chat group you could ask questions regarding the learning content and reading assignments, or share other learning resources, links and even cybersecurity events, interesting podcast episodes or webinars.

This is also the channel that we will use to post any messages or announcements relevant to the course. A **code of conduct** for the chat group will be shared during the orientation seminar.

Here is the link to the Signal website or you can download the app from the official Apple or Android app store: https://signal.org/download/



Signal for Mobile

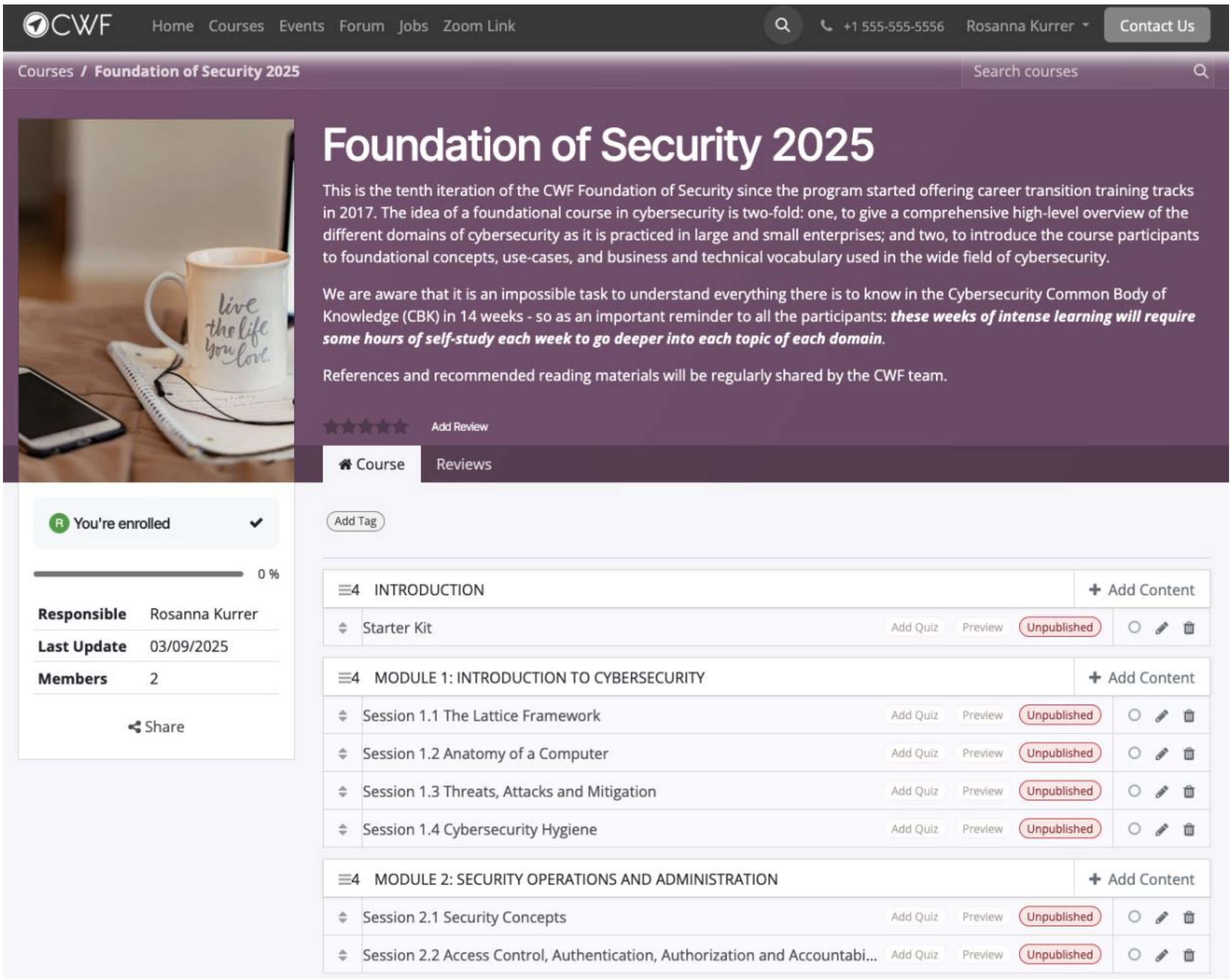
Signal for Desktop

6. LEARNING MANAGEMENT PLATFORM

CWF Learning Management Platform is where all the course work content will be shared.

During the orientation seminar on 27 September, we will do a walkthrough of how to access the platform. Each participant will need an email address to access the learning platform.

Below is an image of the FoS dashboard which shows coursework content (currently unpublished – coursework will be published on a weekly basis).



Foundation of Security 2025

This is the tenth iteration of the CWF Foundation of Security since the program started offering career transition training tracks in 2017. The idea of a foundational course in cybersecurity is two-fold: one, to give a comprehensive high-level overview of the different domains of cybersecurity as it is practiced in large and small enterprises; and two, to introduce the course participants to foundational concepts, use-cases, and business and technical vocabulary used in the wide field of cybersecurity.

We are aware that it is an impossible task to understand everything there is to know in the Cybersecurity Common Body of Knowledge (CBK) in 14 weeks - so as an important reminder to all the participants: ***these weeks of intense learning will require some hours of self-study each week to go deeper into each topic of each domain.***

References and recommended reading materials will be regularly shared by the CWF team.

Responsible	Rosanna Kurrer
Last Update	03/09/2025
Members	2

INTRODUCTION — + Add Content

- Starter Kit — Add Quiz | Preview | Unpublished

MODULE 1: INTRODUCTION TO CYBERSECURITY — + Add Content

- Session 1.1 The Lattice Framework — Add Quiz | Preview | Unpublished
- Session 1.2 Anatomy of a Computer — Add Quiz | Preview | Unpublished
- Session 1.3 Threats, Attacks and Mitigation — Add Quiz | Preview | Unpublished
- Session 1.4 Cybersecurity Hygiene — Add Quiz | Preview | Unpublished

MODULE 2: SECURITY OPERATIONS AND ADMINISTRATION — + Add Content

- Session 2.1 Security Concepts — Add Quiz | Preview | Unpublished
- Session 2.2 Access Control, Authentication, Authorization and Accountabi... — Add Quiz | Preview | Unpublished

7. THE CYBERWAYFINDER TRAINERS TEAM

We encourage you to expand your network of practicing cybersecurity professionals by connecting to all the CWF team of trainers on LinkedIn. Please don't hesitate to send a connection request!

- **Marie Vinck**
https://www.linkedin.com/in/marijkevinck/

- **Patrick Wheeler**
https://www.linkedin.com/in/kpatrickwheeler/

- **Rosanna Kurrer**
https://www.linkedin.com/in/rosannakurrer/

- **Michael Garceau**
https://www.linkedin.com/in/michael-g-b98788/

8. SUGGESTED READING AND OTHER RESOURCES

As we progress, there are also many popular depictions of cybersecurity careers, technologies and topics. If you would like a few recommendations:

- TV series: **"Mr. Robot"** is widely regarded as the best balancing of technical accuracy and storytelling
- TV series: **"Black Mirror"** – explores speculative tech scenarios and the societal impact of emerging technologies, touching on privacy, identity theft, and ethical tech
- Movie: **"The Internet's Own Boy: The Story of Aaron Swartz"** (2014) - interviews, archival footage, and expert commentary, highlighting Swartz's vision for a democratic internet and the challenges of fighting for digital civil liberties
- Movie: **"Snowden"** (2016) - the former NSA contractor who leaked classified information revealing global mass surveillance programs conducted by intelligence agencies
- Book: **"The Cuckoo's Egg"** by Clifford Stoll is a famous first-person account of tracking a hacker who infiltrated the computer system at Lawrence Berkeley National Laboratory in 1986 that is incredibly relevant today
- Book: **"Sandworm"** by Andy Greenberg - An investigative account of a Russian hacking group and the rise of state-sponsored cyberattacks on critical infrastructure
- Newsletter: **Schneier on Security** https://www.schneier.com/crypto-gram/
- Newsletter: **SANS newsletters** https://www.sans.org/newsletters, particularly NewsBites

Additionally various blogs and podcasts will be recommended throughout the course, and you are encouraged to **curate your own favorite information sources** for keeping up to date of current events in the cybersecurity world.

9. YOUR OWN SAFE CYBER JOURNEY

As we work together in this learning journey there are a few things that should be said about the pedagogy and cohort approach. A well-regarded academic model for adult education that helps us differentiate this program from traditional education and university programs is well described in the Knowles Adult Learning framework.

Need to Know: Adults need to know ***why*** they need to learn something and what the benefits will be for them before they fully commit or buy into the learning process. If you are not finding this in the curriculum, please don't hesitate to ask. We know why we have placed the materials for you, but we need your buy-in as well.

Experience: Adults bring with them a wealth of life experiences and trainers should encourage them to share and reflect on those experiences as part of the overall learning process. We want and need your background and experience in cybersecurity. Do not leave your experience behind you in this journey, find the points of relevancy and leverage them.

Self-Concept: This principle acknowledges that adults like to be in control of their learning. And this is integral to how we encourage you to approach these sessions. Although baseline material is presented, you are encouraged to supplement this and discuss in detail your thoughts and reactions to the materials during the virtual seminars.

Readiness to Learn: Adults are reluctant to learn something that has no relevance to their immediate situations, but rather, they're motivated to learn when the training content can directly help them solve current real-life/work problems. This can be a hindrance when we are learning material we are not applying in the workplace immediately. Recognize this early and address it if it starts to become a problem in your engagement with the material.

Problem-Centered Approach: This principle acknowledges that adults tend to be more receptive to learning when they're presented with practical problems and challenges to solve. This is the goal of the virtual seminars, and you are encouraged to dig deeply into these topics in other ways as well.

Intrinsic Motivation: Adult learners are driven by internal motivations like personal growth, career advancement or a sense of accomplishment and achievement. This is **the single most important success factor** we have seen for our students. Finding your **Cyber Why** and ensuring you stay intrinsically motivated to learn and explore the material is the single most important thing. If you find yourself lagging in intrinsic motivation, **talk to us! We can help**.

Psychological Safety is another critical success factor we intend to create in CWF cohorts - for all the cohort members as well as the trainers and coordinators. Maintaining psychological safety requires instructors and participants to be aware of the following key practices:

- Fostering a **welcoming, respectful, and supportive** learning environment where participants feel heard and included. This allows learners to feel secure enough to actively engage in the learning experience.

- Ensuring **positive communication** patterns that are free from sarcasm, cynicism, and judgment. We need to know that all voices matter and we can speak openly.

- Providing **constructive feedback** focused on behaviors rather than personal criticism. Feedback should inspire growth, not feelings of failure or incompetence.

- **Intentionally designing activities** that encourage us to share our experiences and leverage our existing strengths and finding opportunities to validate our prior knowledge.

- **Promoting collaboration** over competition. We learn better together in a community-oriented space, in a path toward collective growth and purpose.

- Cultivating **emotional intelligence and empathy** within the cohort as well as instructors and facilitators. The ability to read the room and respond appropriately helps keep everyone at ease.

From all of us at CyberWayFinder:

We wish you all the best in your learning journey with us and beyond!