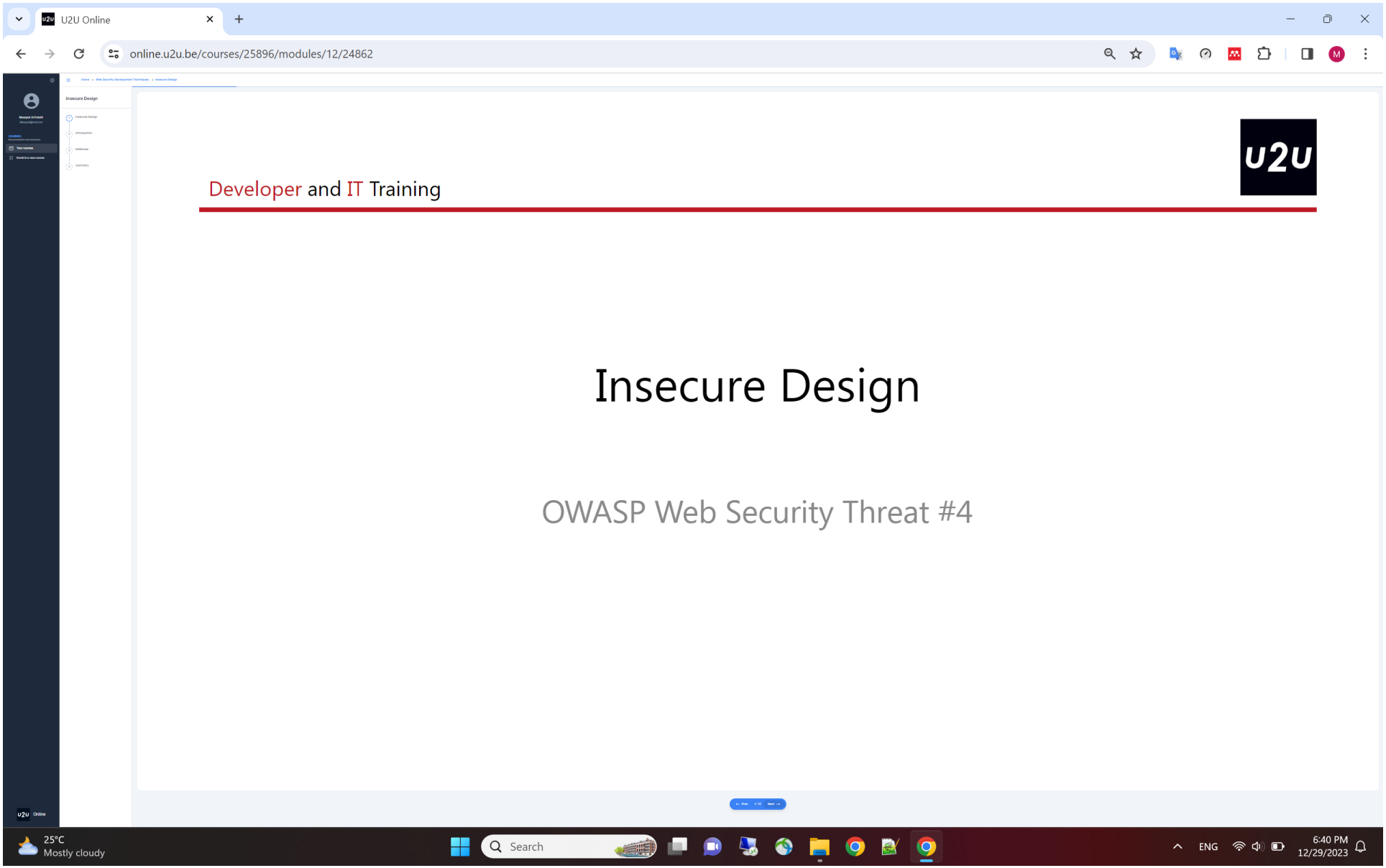
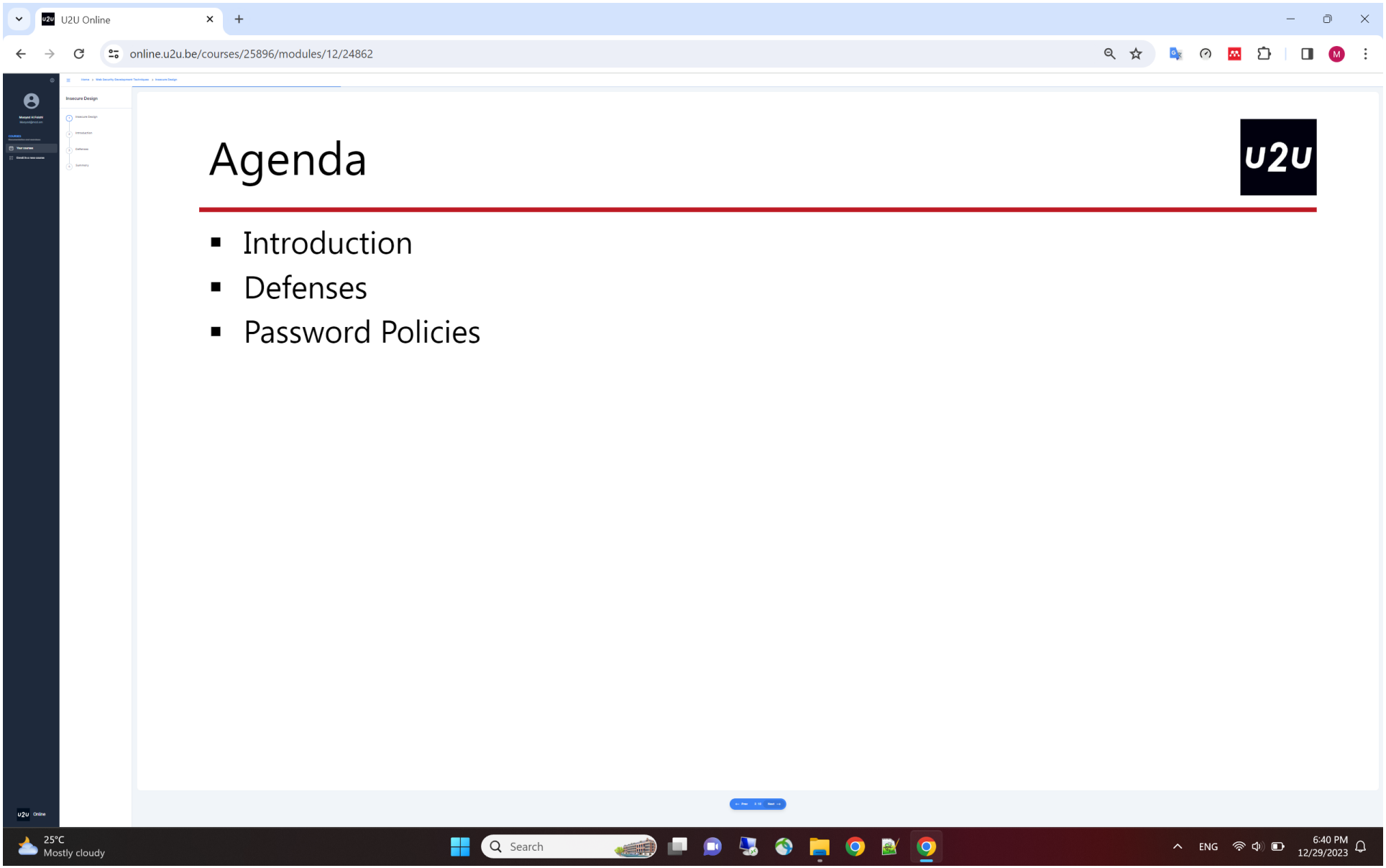
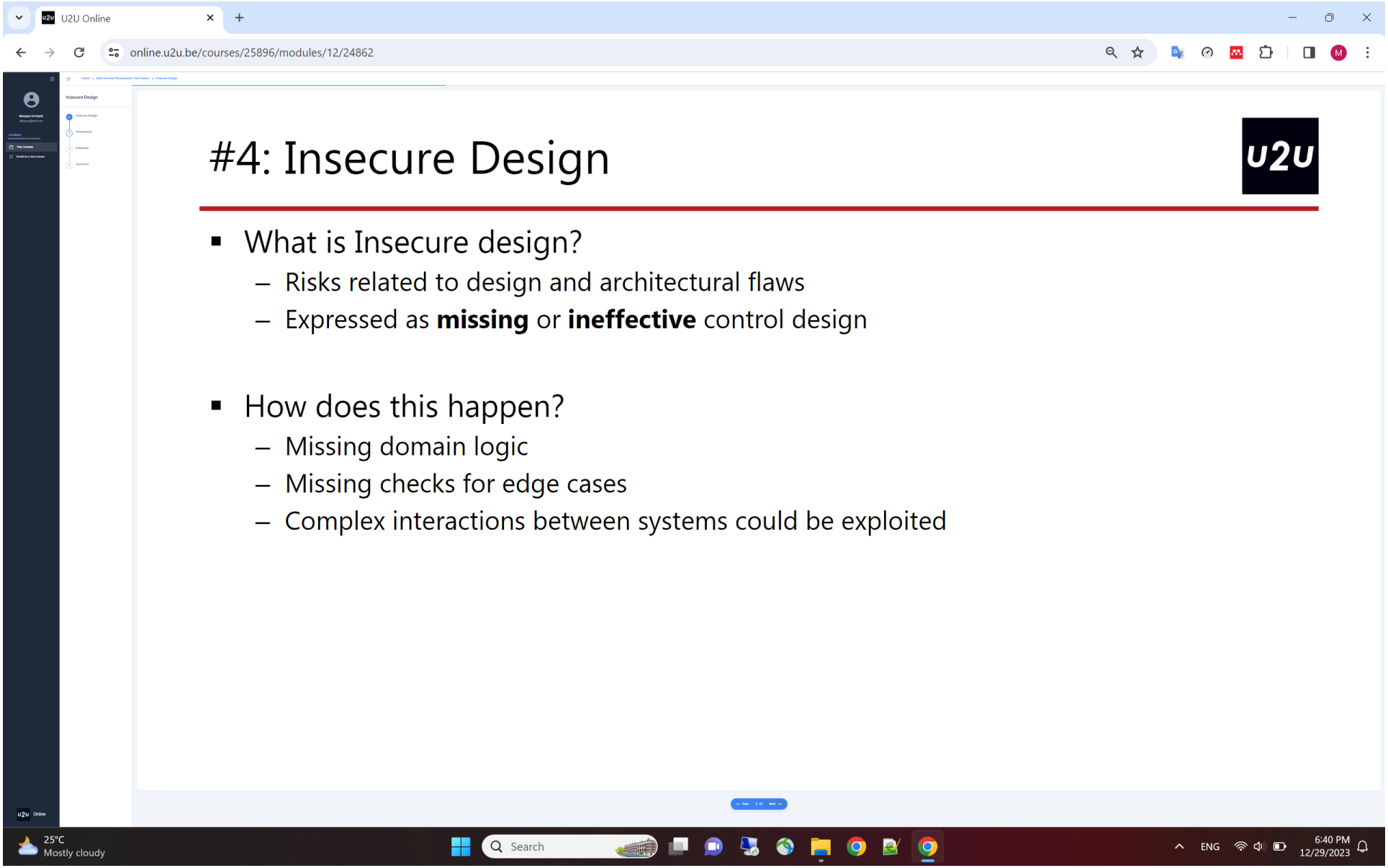
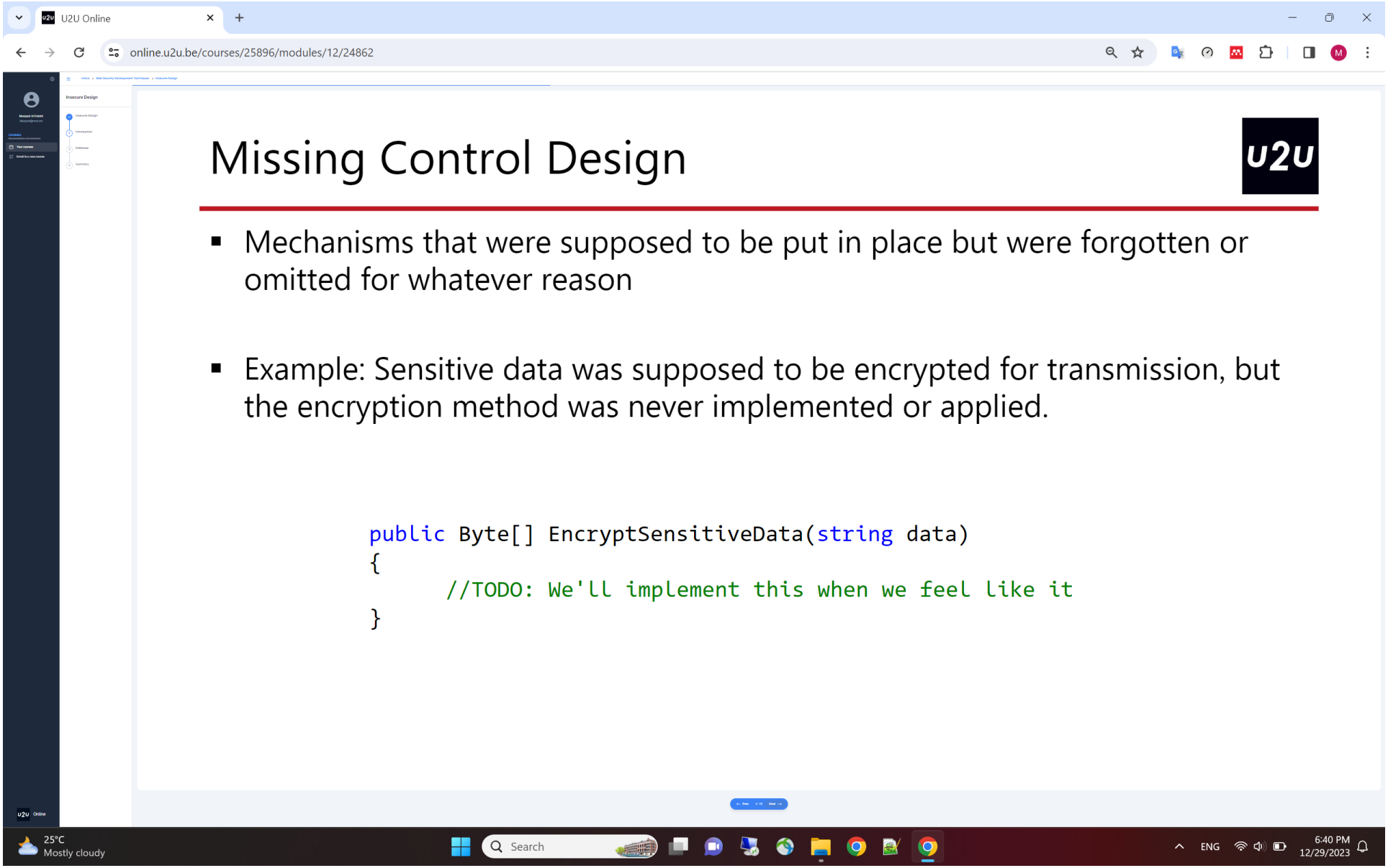

U2U Online
online.u2u.be/courses/25896/modules/12/24862
Insecure Design
Developer and IT Training
U2U
Insecure Design
OWASP Web Security Threat #4
25°C
Mostly cloudy
Search
ENG
6:40 PM
12/29/2023


U2U Online
online.u2u.be/courses/25896/modules/12/24862
Insecure Design
Agenda
u2u
Introduction
Defenses
Password Policies
25°C
Mostly cloudy
Search
ENG
6:40 PM
12/29/2023

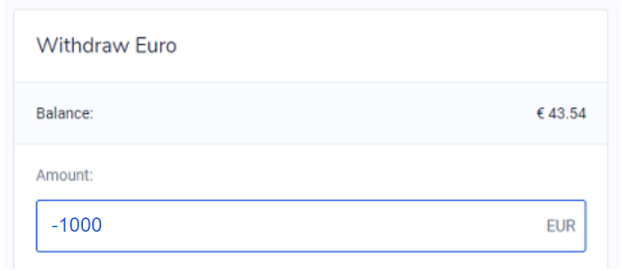

U2U Online
online.u2u.be/courses/25896/modules/12/24862
#4: Insecure Design
u2u
What is Insecure design?
Risks related to design and architectural flaws
Expressed as missing or ineffective control design
How does this happen?
Missing domain logic
Missing checks for edge cases
Complex interactions between systems could be exploited
25°C
Mostly cloudy
Search
ENG
6:40 PM
12/29/2023

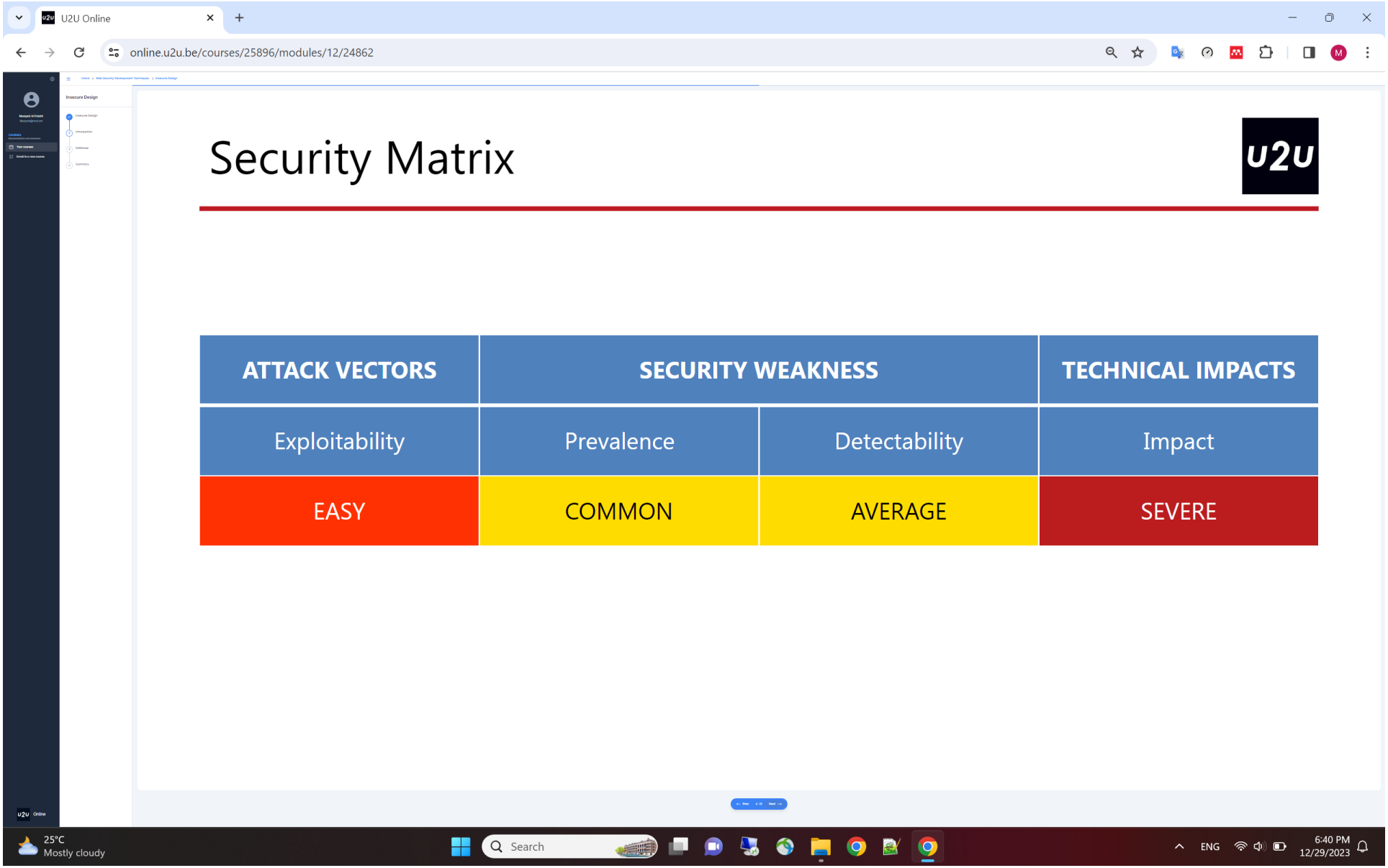

U2U Online
online.u2u.be/courses/25896/modules/12/24862
Insecure Design
Introduction
Defenses
Summary
Missing Control Design
U2U
Mechanisms that were supposed to be put in place but were forgotten or omitted for whatever reason
Example: Sensitive data was supposed to be encrypted for transmission, but the encryption method was never implemented or applied.
public Byte[] EncryptSensitiveData(string data)
{
//TODO: We'll implement this when we feel like it
}
25°C
Mostly cloudy
Search
ENG
6:40 PM
12/29/2023

Ineffective Control Design

- Mechanisms that allow for an attack to happen because of insufficient checks
- Example: a method is supposed to update an account owner's balance after withdrawing money, but it doesn't check the sign of the amount that is being withdrawn

```
public void Withdraw(decimal amount)
{
  this.balance -= amount;
}
```




U2U Online
online.u2u.be/courses/25896/modules/12/24862
Insecure Design
Security Matrix
u2u
ATTACK VECTORS
SECURITY WEAKNESS
TECHNICAL IMPACTS
Exploitability
Prevalence
Detectability
Impact
EASY
COMMON
AVERAGE
SEVERE
25°C
Mostly cloudy
Search
ENG
6:40 PM
12/29/2023

U2U Online

online.u2u.be/courses/25896/modules/12/24862

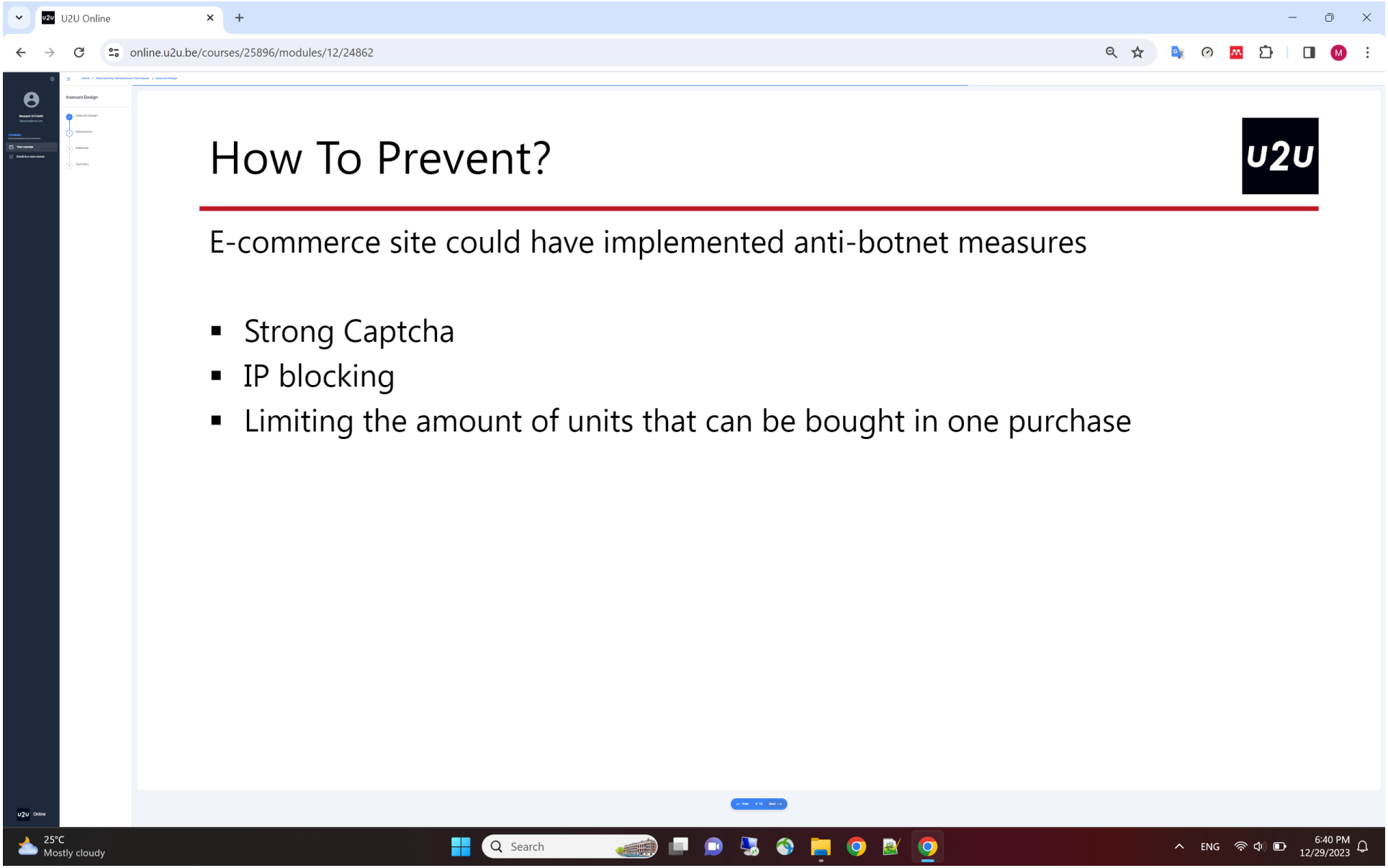
Example Scenarios

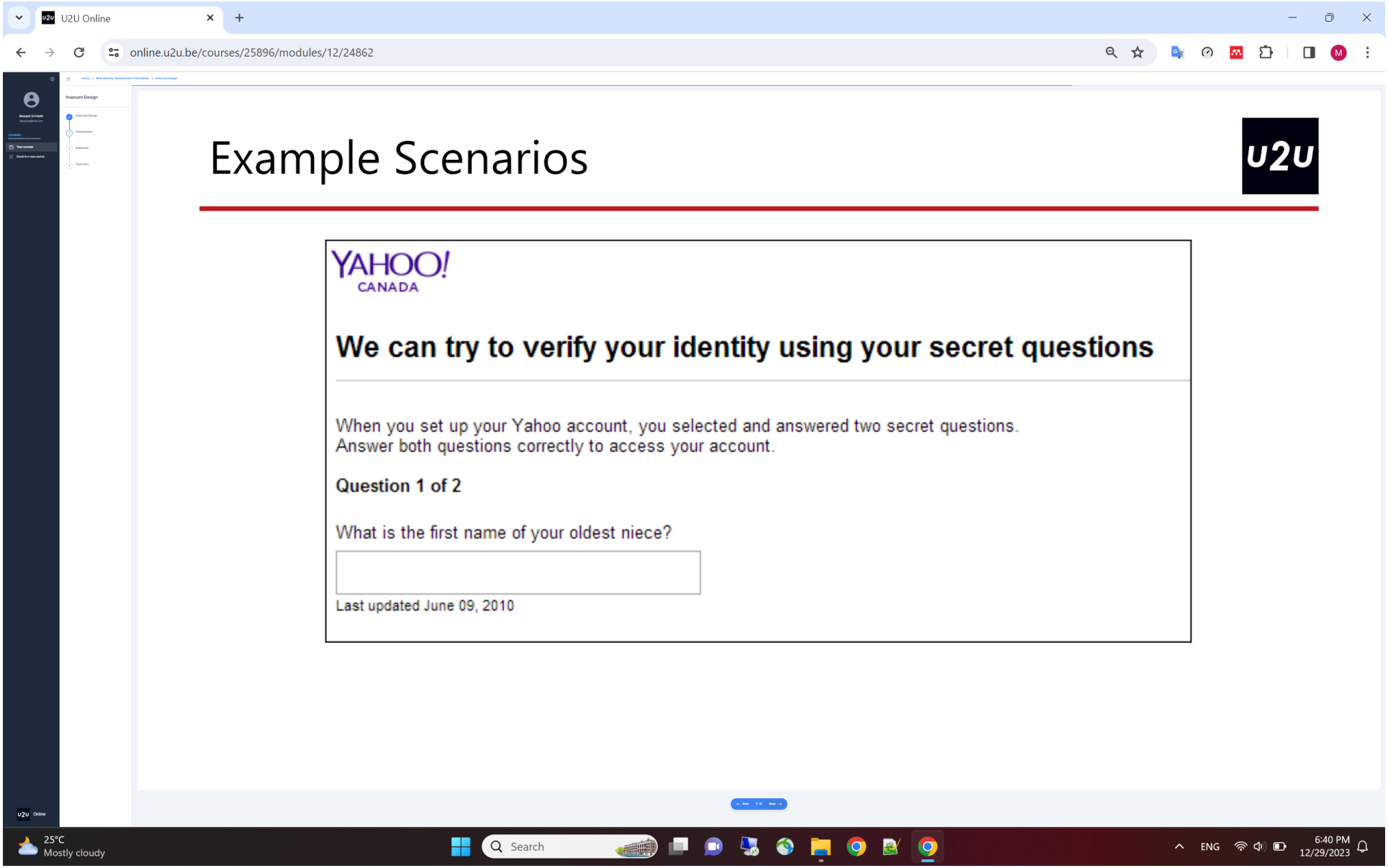
- New video card or gaming console is released
- E-commerce sites allow botnets to buy all available units
- Scalpers use these botnets to create scarcity and drive up price
- Both hardware manufacturer and e-commerce site suffer terrible publicity

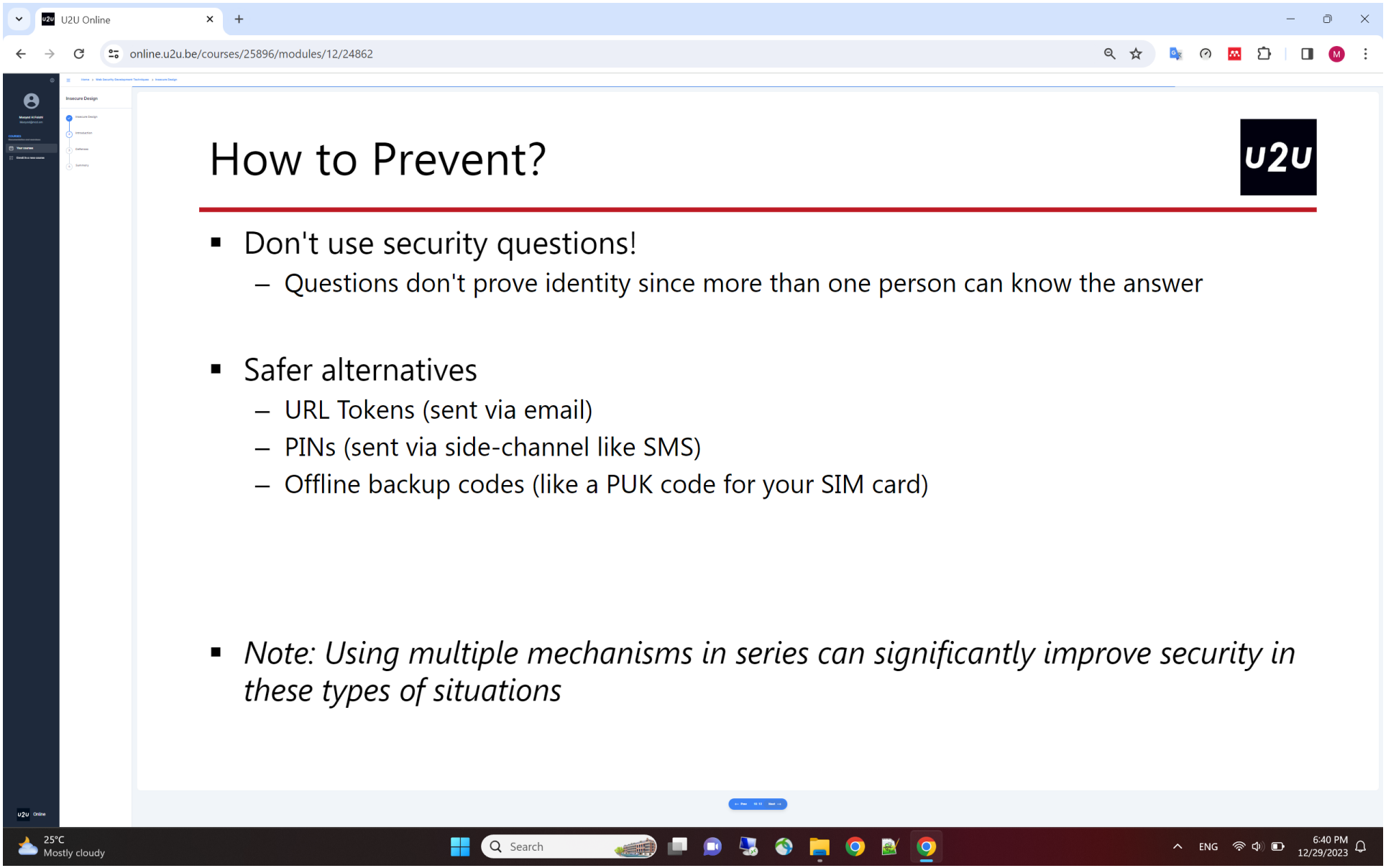
25°C Mostly cloudy

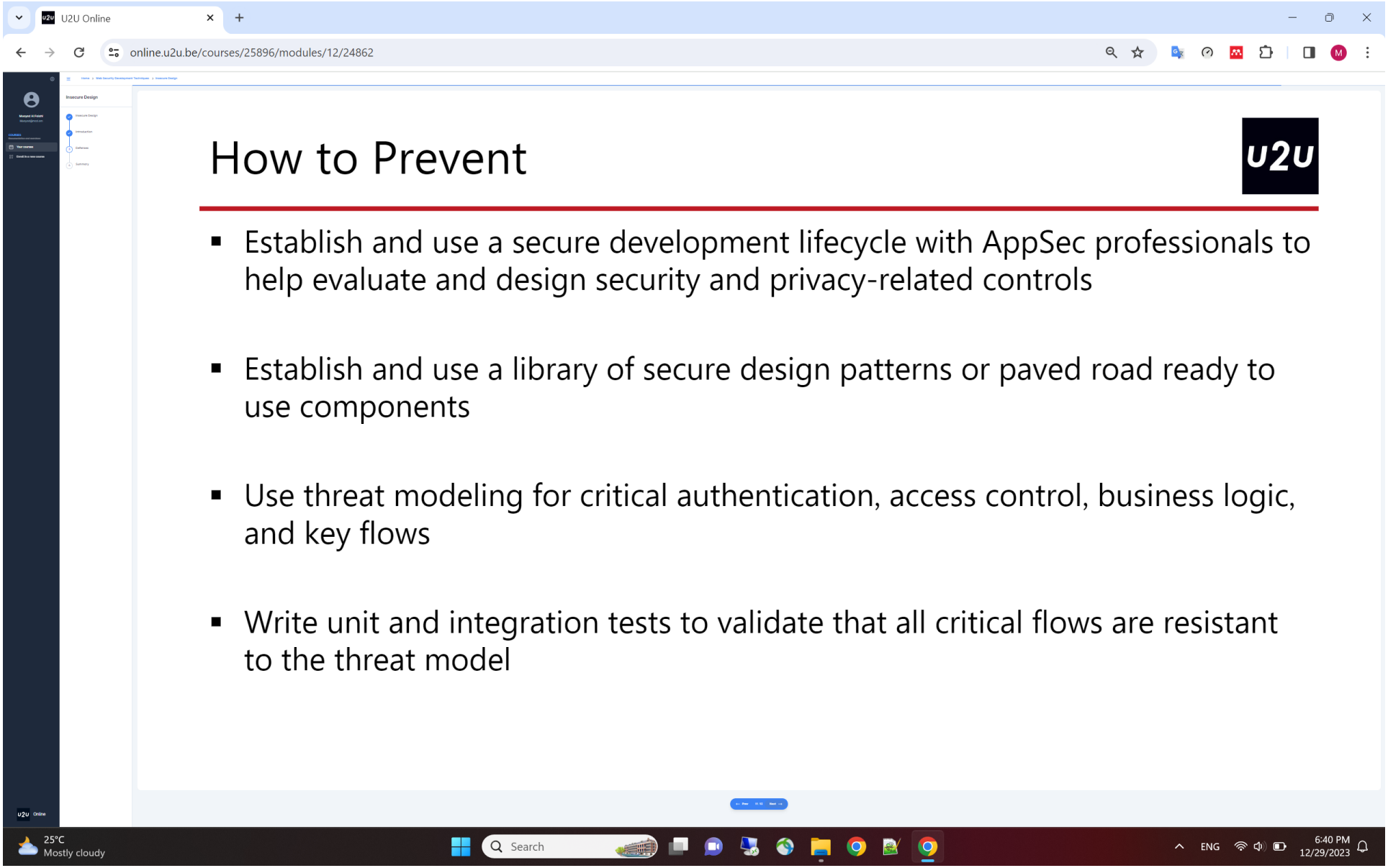
Search

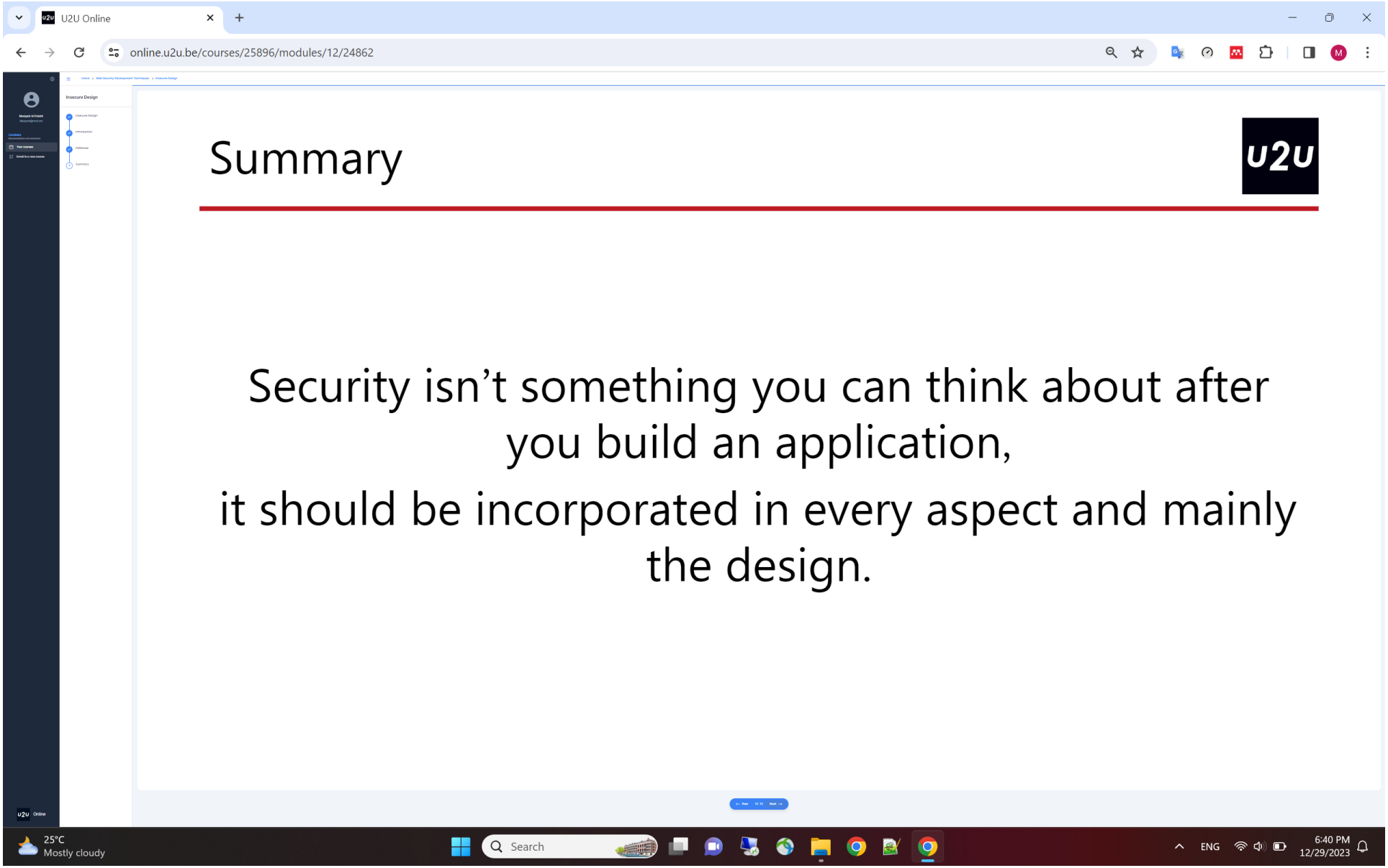
ENG 6:40 PM 12/29/2023


U2U Online
online.u2u.be/courses/25896/modules/12/24862
Insecure Design
How To Prevent?
u2u
E-commerce site could have implemented anti-botnet measures
Strong Captcha
IP blocking
Limiting the amount of units that can be bought in one purchase
25°C
Mostly cloudy
Search
ENG
6:40 PM
12/29/2023


U2U Online
online.u2u.be/courses/25896/modules/12/24862
Insecure Design
Introduction
Defenses
Summary
Example Scenarios
u2u
YAHOO!
CANADA
We can try to verify your identity using your secret questions
When you set up your Yahoo account, you selected and answered two secret questions.
Answer both questions correctly to access your account.
Question 1 of 2
What is the first name of your oldest niece?
Last updated June 09, 2010
25°C
Mostly cloudy
Search
ENG
6:40 PM
12/29/2023


U2U Online
online.u2u.be/courses/25896/modules/12/24862
Insecure Design
How to Prevent?
u2u
Don't use security questions!
– Questions don't prove identity since more than one person can know the answer
Safer alternatives
– URL Tokens (sent via email)
– PINs (sent via side-channel like SMS)
– Offline backup codes (like a PUK code for your SIM card)
Note: Using multiple mechanisms in series can significantly improve security in these types of situations
25°C
Mostly cloudy
Search
ENG
6:40 PM
12/29/2023


U2U Online
online.u2u.be/courses/25896/modules/12/24862
How to Prevent
U2U
Establish and use a secure development lifecycle with AppSec professionals to help evaluate and design security and privacy-related controls
Establish and use a library of secure design patterns or paved road ready to use components
Use threat modeling for critical authentication, access control, business logic, and key flows
Write unit and integration tests to validate that all critical flows are resistant to the threat model
25°C
Mostly cloudy
Search
ENG
6:40 PM
12/29/2023


U2U Online
online.u2u.be/courses/25896/modules/12/24862
Insecure Design
Summary
U2U
Security isn't something you can think about after you build an application,
it should be incorporated in every aspect and mainly the design.
25°C
Mostly cloudy
Search
ENG
6:40 PM
12/29/2023