



**Workshop:**

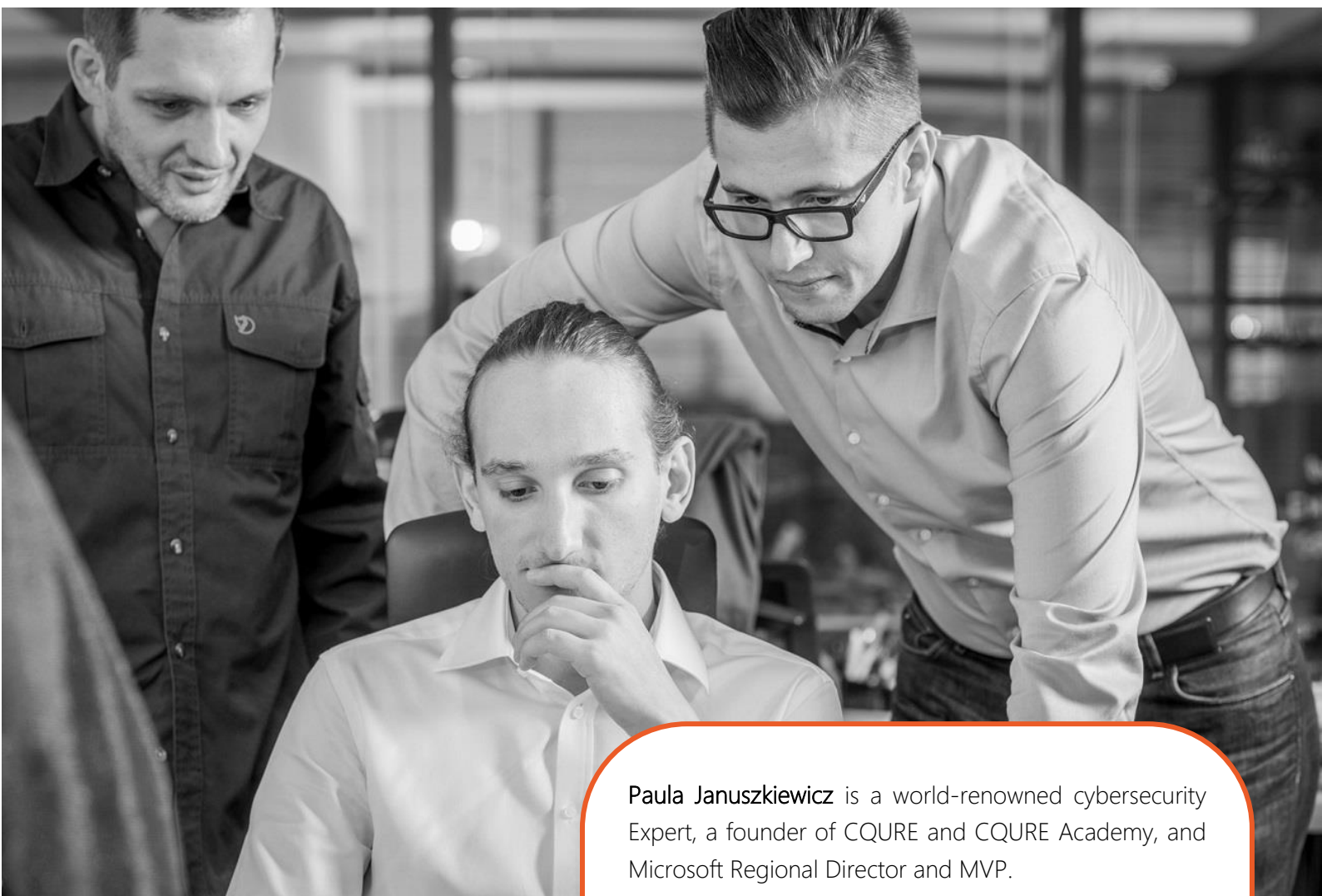
# Hacker's Perspective on Remote Working

**CQURE**  
Warsaw New York Dubai Zug

[info@cquire.pl](mailto:info@cquire.pl)

[www.cquire.pl](http://www.cquire.pl)  
[www.cquireacademy.com](http://www.cquireacademy.com)

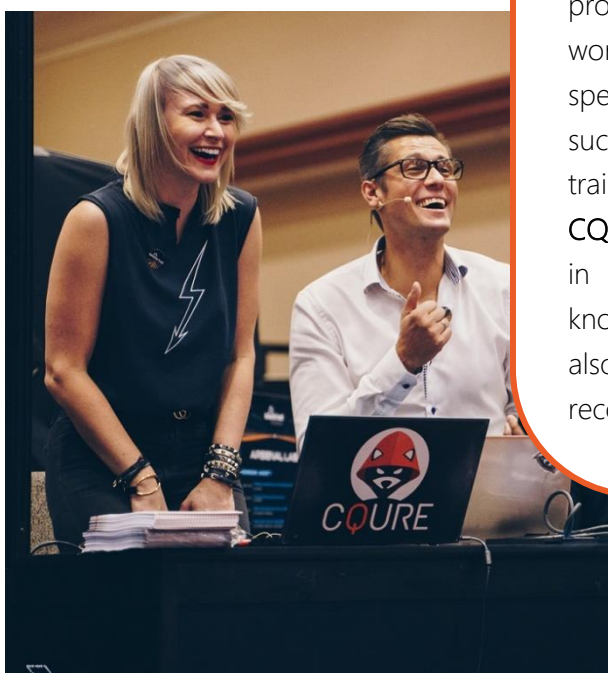




**Paula Januszkiewicz** is a world-renowned cybersecurity Expert, a founder of CQURE and CQURE Academy, and Microsoft Regional Director and MVP.

**CQURE Academy** focuses on cybersecurity training program consisting of over high-quality 20 technical workshops and seminars and providing certification to specialists. Additionally, in October 2016 CQURE has successfully launched online and subscription-based training.

**CQURE Experts** speak at international events and engage in multiple cybersecurity projects – they bring their knowledge and experience to trainings. CQURE Academy also involves R&D – that is why CQURE Team is recognizable in the cybersecurity field.



## Introduction

Nowadays, secure home office solutions and procedures are essential for maintaining business continuity. As remote working is getting more and more popular, cybercriminals are looking for opportunities to put their hands on the corporate data – to sell them, extort ransom, leak them or use in other malicious ways.

During this workshop you will become familiar with **the hackers' perspective on the remote working** and many different situations hackers can create and exploit to be able to access company's information. You will also learn how to avoid mistakes and what solutions and approaches companies can implement to make the home office a safer workplace.

You will learn not only what are the most crucial risks and **threats related with remote workplace** but also how technology and proper procedures will help you in mitigating those. This workshop will be very **demo intense** with loads of **real-life examples** coming directly from CQURE's experience.



**Paula says:** *Pure coolness with a value! This workshop shows how to simple mistakes and quick changes may destroy whole enterprise security. It is great to learn from other people's mistakes, right?*

### Audience

IT management, IT department employees, IT professionals and other people responsible for planning network and perimeter security.

### Materials

Authors' unique tools, presentation slides with notes, workshop instructions.

### Certification

At the end participants will receive the online Certificate of attendance signed by the CQURE Speaker.

## Agenda

### Module 1: Overview of the Modern Threats

1. What are the attacker's motivations?
2. What is the target?

### Module 2: Phishing

3. What are "phishing" and "spear phishing"?
4. Typosquatting – URL Hijacking
5. How to spot a phishing attempt (in e-mail and on the web)?

### Module 3: Remote workplace access

1. Using company e-mail at home
2. Remote desktop attacks
3. Risks of utilizing corporate VPN

### Module 4: Passwords

1. Password vs. Passphrase
2. Password reusing
3. Saving passwords
4. Password ManagersBroker (CASB)

### Module 5: How to protect remote work users

1. Anti-phishing solutions (ATP, SafeLinks, Smart Screen)
2. Exploit Guard (ASR)
3. Data Leak Prevention
4. Multi-Factor Authentication (MFA) and Windows Hello for Business (WHfB)
5. Conditional access.

