



CYBER WARDEN

PRACTICAL CYBER RISK MANAGEMENT

Understanding Business Email Compromise (BEC)

PROTECTING YOUR ORGANIZATION FROM EMAIL SCAMS

Andrew MacLachlan

November 2024

Introduction to BEC

- ▶ Definition: A type of cybercrime where attackers use email to trick individuals into transferring money or divulging sensitive information.
 - ▶ <https://www.fbi.gov/how-we-can-help-you/scams-and-safety/common-frauds-and-scams/business-email-compromise>
 - ▶ <https://www.microsoft.com/en-us/security/business/security-101/what-is-business-email-compromise-bec>
- ▶ One of the most financially damaging online crimes.
- ▶ Email is the starting point for 91 percent of cyberattacks.
- ▶ Upto 80% increase in some sectors in the last year
 - ▶ <https://abnormalsecurity.com/blog/manufacturing-industry-email-attack-trends>

How BEC Works

- ▶ Common Tactics:
 - ▶ Spoofing email addresses
 - ▶ Spearphishing emails
 - ▶ Using Malware to gain access
- ▶ Examples:
 - ▶ Fake invoices
 - ▶ CEO fraud asking for urgent transfers

Warning Signs of BEC

- ▶ Unusual payment requests
- ▶ Changes in payment procedures
- ▶ Urgent or confidential requests
- ▶ Aggression (do it or else...)
 - ▶ Threats of legal action
 - ▶ Threats to employment
 - ▶ Usually linked to urgency of action

Prevention Tips

- ▶ Use multi-factor authentication (MFA)
- ▶ Educate employees about phishing
- ▶ Implement strict controls around payments
 - ▶ Two person approval
 - ▶ Confirm with a phone call to the person supposedly making the request
 - ▶ Don't use the contact details from the received email
- ▶ Implement an email scanning solution
- ▶ Implement DMARC

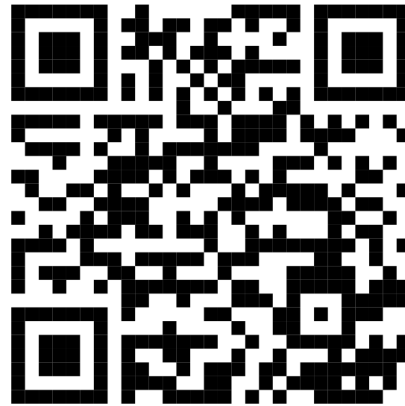
What to Do If You Suspect BEC

- ▶ Report to IT/security team
- ▶ Don't make any irregular payments without confirmation
- ▶ If a payment has been made, immediately contact the bank to stop/reverse the payment
- ▶ Don't delete any communications
- ▶ Report to the police

Contact Details



Andrew's LinkedIn



Cyber Warden LinkedIn



Andrew's Contact

Download a copy of these slides

