Interview Transcript: Cybersecurity Practices in Small Hotels(1)

Interviewer:

OK, we're starting the interview. The research title is *The Impact of Employee Cybersecurity Awareness and Small Hotel Security*. The purpose of the study is to explore how employee cybersecurity awareness influences security in small hotels. Your participation helps us assess the effectiveness of cybersecurity training and enhance hotel security. Participation involves completing an interview, with data used solely for academic research on cybersecurity trends and attitudes. Withdrawal is permitted at any time without penalty. Data will be confidential, anonymized, and stored in compliance with GDPR standards. The research team will have access to the data with no personal identifiers published. Data is used for research purposes in a research paper on hotel security, potentially published in academic journals. Participation is voluntary. Do I have your verbal consent?

Respondent:

Yes, I agree.

Interviewer:

Great. Then we can start. Let’s talk about your general experience with training. Can you describe any cybersecurity training you've received at the hotel where you work?

Respondent:

Yeah, sure. I received basic cybersecurity training as part of my onboarding process. It covered essential topics like protecting customer data and the secure use of the hotel's booking system. However, the training felt more like a formality than something deeply relevant to my role.

Highlighted for thematic analysis: Lack of perceived relevance and formal nature of training.

Interviewer:

How often do you participate in training sessions? Are they yearly, monthly, or weekly?

Respondent:

In the past year, I have only had one formal training session. There haven't been any follow-up or refresher courses.

Highlighted for thematic analysis: Infrequency of training.

Interviewer:

What topics were covered in the training? Was it phishing, secure passwords, or data protection?

Respondent:

The main focus was on password management, recognizing phishing emails, and protecting guest personal data. There was also a brief mention of secure Wi-Fi practices, but nothing detailed.

Highlighted for thematic analysis: Content of training (focus on basics, lack of depth in Wi-Fi security).

Interviewer:

How well do you think the training prepared you to handle cybersecurity trends?

Respondent:

Honestly, I don't think it was thorough enough. While I learned the basics, I don't feel fully confident dealing with complex cybersecurity issues, especially in urgent situations like a breach or an attempted scam.

Highlighted for thematic analysis: Lack of preparedness and confidence in dealing with complex threats.

Interviewer:

How was the training delivered? Was it online, in person, a workshop, or group training?

Respondent:

The training was delivered online. It consisted mostly of video modules that we had to watch, followed by a short quiz. It was convenient, but it lacked interactivity, which made it less engaging.

Highlighted for thematic analysis: Online delivery and lack of engagement due to non-interactive format.

Interviewer:

Did you find the training easy to understand and follow?

Respondent:

Yes, the materials were straightforward, but I think they could have been more detailed, especially for night shifts where I'm alone and have to handle issues by myself.

Highlighted for thematic analysis: Need for more detailed, role-specific training for night shifts.

Interviewer:

Do you feel the training was relevant to your specific job responsibilities?

Respondent:

To some extent, yes. Password management and phishing were definitely relevant. However, the training didn't cover certain situations I face, like suspicious phone calls or securing guest Wi-Fi networks.

Highlighted for thematic analysis: Limited role-specific relevance of training.

Interviewer:

How do you stay informed about new cybersecurity threats or best practices? Does your hotel provide them?

Respondent:

Not really. I think more focus on social engineering attacks, specifically how scammers might try to manipulate night staff when they're alone, would have been

useful.

Highlighted for thematic analysis: Lack of ongoing updates and focus on night-shift-specific threats.

Interviewer:

How engaged were you during the training? Was it boring, or was it well delivered?

Respondent:

To be honest, it wasn't very engaging. The training felt generic and wasn't tailored to the challenges I face as a night receptionist. It would have been more effective if it included real-life scenarios or interactive elements.

Highlighted for thematic analysis: Generic content and lack of interactivity reducing engagement.

Interviewer:

Do you feel motivated to follow cybersecurity practices in your daily work? Why or why not?

Respondent:

Yes, I'm motivated because I know cybersecurity is important for protecting guest information. But I wish the training had made it clearer how my actions can directly impact security.

Highlighted for thematic analysis: Motivation vs. lack of clarity on impact.

Interviewer:

Were there any challenges or difficulties you faced during the training?

Respondent:

The main challenge was that the training wasn't engaging. It felt like a "check-the-box" exercise rather than something that prepared me for real-world threats.

Highlighted for thematic analysis: "Check-the-box" nature of training and lack of practical application.

Interviewer:

What could be done to make the training more effective or useful for you?

Respondent:

More interactive elements, like simulators or case studies showing actual cyber threats in the hotel environment, would make a huge difference. Also, having someone available for a Q&A session after the training could help clarify things.

Highlighted for thematic analysis: Suggestions for improvement (interactivity, real-life examples, Q&A).

Interviewer:

Have you encountered any cybersecurity issues at work? Any stories?

Respondent:

Yes, I once received a suspicious email asking for guest booking data. It looked really suspicious. The training helped me recognize it as a phishing attempt, so I didn't respond and reported it to a manager. However, I didn't know what the next steps were, and there wasn't any follow-up guidance from the hotel.

Highlighted for thematic analysis: Real-life application and lack of follow-up procedures.

Interviewer:

If you could suggest improvements to the hotel's cybersecurity training, what would they be?

Respondent:

More frequent and engaging sessions, perhaps quarterly, that cover real-life scenarios we could face. It would also help if there was more specific guidance for night staff who might be more vulnerable to certain types of attacks.

Highlighted for thematic analysis: Recommendation for frequency, engagement, and night-shift-specific training.

Interviewer:

Do you think regular cybersecurity training would help prevent potential security issues at your hotel?

Respondent:

Absolutely. Regular training would keep us informed of the latest threats and make us more confident in handling them. It would also create a stronger culture of awareness and responsibility.

Highlighted for thematic analysis: Impact of regular training on confidence and security culture.

Interviewer:

That's it. Thank you so much for participating.

Respondent:

Thank you. Nice talking to you. Bye.
