

Interview Transcript: Cybersecurity Practices in Small Hotels(3)

Respondent:

Good afternoon, my name is —. I'll be talking about my experience with cybersecurity training at the hotel. Most of our cybersecurity training is done online through courses provided by the hotel's interface. I don't remember exactly how often it occurs, but we get a refresher course about **once a year**. The training covers things like **confidentiality, anti-phishing, secure and unsecure practices, password protection, and safeguarding devices that connect to the Internet**.

The training helps build awareness, especially for employees who might not be familiar with electronics or online security. It's good for giving a basic understanding of **cybersecurity practices**.

Highlighted for thematic analysis: Annual refresher schedule, focus on basic awareness topics (confidentiality, anti-phishing, password security).

The training is online, and it's **easy to understand and follow**. There wasn't anything particularly challenging about it. The course includes some job-specific details since we handle sensitive information, like guest details, through emails and phone calls. However, we don't get frequent updates on new threats; I assume these are addressed in the next annual training cycle.

Highlighted for thematic analysis: Online format, ease of use, job relevance for handling sensitive data, lack of timely updates.

The training is **somewhat interactive**, involving reading, answering questions, and fitting puzzle pieces. Personally, I don't feel strongly motivated about daily cybersecurity practices—it's just part of the protocol. We follow these protocols as part of the job. I haven't faced any challenges during training; everything is clear and straightforward.

Highlighted for thematic analysis: Interactivity in training format, low personal motivation, procedural nature of cybersecurity tasks.

I haven't encountered any security incidents at work, and there hasn't been any additional training or guidance outside of the annual refresher. While the hotel could perhaps improve some aspects, I think the current security measures are well-managed. For example, our computers are locked down, so we can't easily put the system at risk. Most security risks would only affect personal accounts, but as long as we follow the protocols, we should be fine.

Regular cybersecurity training could definitely help prevent potential issues for the hotel in the future.

Highlighted for thematic analysis: Absence of security incidents, limited additional guidance, reliance on locked systems and protocols, support for regular training as a preventive measure.