Future research

🔎 7: Future Research

Despite these findings, several avenues remain open for future research to deepen our understanding of how employee cybersecurity awareness affects the overall security of small hotels:

1. **Longitudinal Studies on Training Effectiveness**

   While the current research highlights optimal training frequencies, future studies could employ longitudinal designs to examine how adherence evolves over extended periods. This approach would shed light on whether quarterly or biannual training continues to be effective, or if additional “refreshers” are needed to maintain high compliance levels (Afolabi, 2024).

2. **Cost-Benefit Analysis of Cybersecurity Investments**

   Many small hotels struggle with budget constraints, which makes it critical to evaluate the return on investment (ROI) of cybersecurity training programs. Future research could explore detailed cost-benefit analyses, factoring in variables such as reduced downtime, avoidance of data breaches, and increased customer trust.

3. **Impact of Emerging Technologies**

   As more hotels implement IoT devices (e.g., smart locks, digital key systems), new attack vectors emerge. Further research could investigate how training programs should adapt to cover these specialized threats and whether emerging technologies—like AI-driven threat detection—can be leveraged cost-effectively by smaller establishments (Chin, n.d.).

4. **Gamification and Innovative Training Methods**

   Although this study underscores the value of interactive sessions, further exploration could assess gamification techniques, virtual reality simulations, or mobile app-based learning. Evaluating whether these innovative methods improve retention and practical skills, compared to traditional or scenario-based training, would offer

valuable insights into optimizing engagement (Kahraman et al., 2021).

5. **Cross-Cultural and Global Comparative Studies**

   Cybersecurity norms and regulatory frameworks can differ significantly by region. A comparative study across different countries or cultures would help determine whether training methods need to be localized. This could also illuminate how varying legal requirements (e.g., GDPR in Europe versus other data protection regimes) influence the perception and efficacy of training.

6. **Integration with Organizational Culture and Policy**

   Future work could focus on how broader organizational strategies—such as leadership support, internal communication, and reward systems—affect cybersecurity awareness. Exploring the interplay between a hotel's overall culture and the success of cybersecurity initiatives would help clarify best practices for management-led interventions (Negussie, 2023).

7. **Measuring Behavioral Change Beyond Awareness**

   Although awareness is a crucial first step, future research might delve into how behavioral metrics—like the frequency of reporting phishing emails, adherence to password policies, or responding to simulated attacks—correlate with different training interventions. This emphasis on actual behaviour, rather than self-reported knowledge, can provide more robust evidence of training impact (UpGuard, 2024).

By pursuing these research directions, stakeholders can more precisely tailor cybersecurity solutions to the realities of small hotels. Comprehensive, ongoing investigations will also facilitate the development of evolving best practices, ensuring that these businesses remain equipped to counter emerging cyber threats.

🔍 Overleaf format:

\section{Future Research}

Despite these findings, several avenues remain open for future research to deepen
our understanding of how employee cybersecurity awareness affects the overall security
of small hotels:

\begin{enumerate}
\item \textbf{Longitudinal Studies on Training Effectiveness.}

While the current research highlights optimal training frequencies, future studies could employ longitudinal designs to examine how adherence evolves
over extended periods. This approach would shed light on whether quarterly or
biannual training continues to be effective, or if additional ``refreshers'' are
needed to maintain high compliance levels \cite{afolabi2024}.

```
\\item \\textbf{Cost-Benefit Analysis of Cybersecurity
Investments.}
Many small hotels struggle with budget constraints, wh
ich makes it critical
to evaluate the return on investment (ROI) of cybersec
urity training programs.
Future research could explore detailed cost-benefit an
alyses, factoring in
variables such as reduced downtime, avoidance of data
breaches, and increased
customer trust.

\\item \\textbf{Impact of Emerging Technologies.}
As more hotels implement IoT devices (e.g., smart lock
s, digital key systems),
```

```
new attack vectors emerge. Further research could inve
stigate how training programs
should adapt to cover these specialized threats and wh
ether emerging technologies---like
AI-driven threat detection---can be leveraged cost-eff
ectively by smaller establishments
\\cite{chinND}.

\\item \\textbf{Gamification and Innovative Training M
ethods.}
Although this study underscores the value of interacti
ve sessions, further
exploration could assess gamification techniques, virt
ual reality simulations,
or mobile app-based learning. Evaluating whether these
innovative methods
improve retention and practical skills, compared to tr
aditional or
scenario-based training, would offer valuable insights
into optimizing engagement
\\cite{kahraman2021}.

\\item \\textbf{Cross-Cultural and Global Comparative
Studies.}
Cybersecurity norms and regulatory frameworks can diff
er significantly by region.
A comparative study across different countries or cult
ures would help determine
whether training methods need to be localized. This co
uld also illuminate how
varying legal requirements (e.g., GDPR in Europe versu
s other data protection
regimes) influence the perception and efficacy of trai
ning.

\\item \\textbf{Integration with Organizational Cultur
```

```
e and Policy.}
Future work could focus on how broader organizational
strategies---such as
leadership support, internal communication, and reward
systems---affect
cybersecurity awareness. Exploring the interplay betwe
en a hotel’s overall
culture and the success of cybersecurity initiatives w
ould help clarify best
practices for management-led interventions \\cite{negu
ssie2023}.

\\item \\textbf{Measuring Behavioral Change Beyond Awa
reness.}
Although awareness is a crucial first step, future res
earch might delve into how
behavioral metrics---like the frequency of reporting p
hishing emails, adherence
to password policies, or responding to simulated attac
ks---correlate with
different training interventions. This emphasis on act
ual behavior, rather than
self-reported knowledge, can provide more robust evide
nce of training impact
\\cite{upguard2024}.
```

\end{enumerate}

By pursuing these research directions, stakeholders can more precisely tailor
cybersecurity solutions to the realities of small hotels. Comprehensive, ongoing
investigations will also facilitate the development of evolving best practices,
ensuring that these businesses remain equipped to counter emerging cyber threats.