サイバー防犯通信

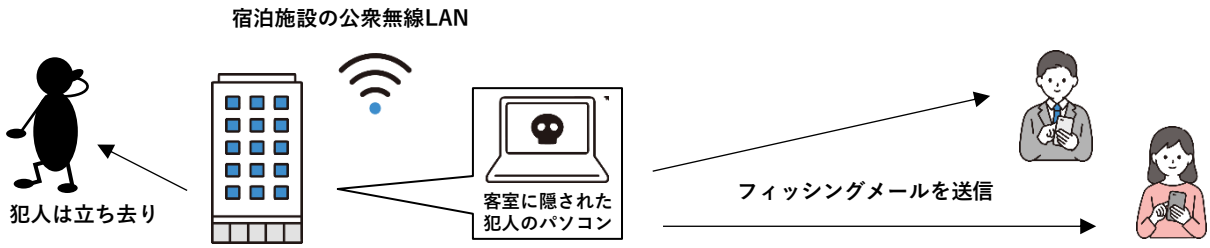
https://www.police.pref.hyogo.lg.jp/cyber/

令和８年３０号
兵庫県警察サイバーセンター
サイバー情報発信室

公衆無線LANからフィッシングメールが大量送信!?

事件の概要

犯人が、宿泊施設客室内のコンセントを使用してパソコンを隠して設置し、宿泊施設の公衆無線LANに接続してフィッシングメールを送信した事件です。



物理的な防止策

01　宿泊者の確実な身分確認

チェックイン時の身分証を確認する。

02　不審な機器の発見

客室設備裏も含めて不審な残置物がないか確認する。備品シールなどで判別できるようにする。

03　コンセント差込口の確認

備品以外の機器が客室内のコンセント差込口を使用していないか確認する。

公衆無線LANのセキュリティ対策

- ☐ 01　業務用ネットワークと分離していますか？
- ☐ 02　安全な管理パスワードを設定し、適切に管理していますか？
- ☐ 03　機器のソフトウェアを最新の状態にしていますか？
- ☐ 04　メーカーによるサポートやアップデートが終了した古い機器をそのまま使い続けていませんか？
- ☐ 05　誰が接続したか、確認・記録できるようになっていますか？
- ☐ 06　宿泊者同士が、お互いの端末にアクセスできない設定になっていますか？
- ☐ 07　宿泊者にネットワークを圧迫するような大容量の動画配信サービス・オンラインゲーム・ファイル共有サイトなどをさせず、また悪意あるサイトアクセスさせないようにDNSフィルタリングを設定していますか？
- ☐ 08　機器のセキュリティ規格を、最新のWPA3にしていますか？
- ☐ 09　宿泊者が正しい公衆無線LANに接続できるよう、わかりやすく案内していますか？
- ☐ 10　公衆無線LANを悪用して、認証のない迷惑メールなどを送信されないようにするための設定（OP25B）をしていますか？
- ☐ 11　使っていない通信の入口（ポート）を閉じたり、通信が集中しすぎないよう、通信量や通信速度を制限していますか？
- ☐ 12　公衆無線LANの共通パスワードを定期的に変更していますか？

サイバーセンター公式「X」(旧Twitter)

兵庫県警察サイバーセンターではX（旧Twitter）で、サイバー犯罪やサイバーセキュリティの情報をいちはやくお届けしています。

https://x.com/HPP_c3division