POLICE - ALERT

Scams targeting hospitality sector

Analysis of crime reports by the National Fraud Intelligence Bureau reveals that the hospitality sector is increasingly being targeted by criminals impersonating IT providers.

Typically, fraudsters will call restaurants and hotels purporting to be a representative of the company that provides their reservation or booking system. The criminals will try to convince the employee to reveal their login details, often under the guise that it's required in order to complete an important software installation.

Once an attacker gains access to a business' computer systems, they'll steal any customer data they come across, this will often include databases of customer names and contact details. This data will then be used to perpetrate targeted phishing scams that are highly convincing. For example, victims have reported receiving calls from people impersonating a restaurant or hotel they have a reservation with. The caller requests a payment from the victim claiming that it's required in order to confirm their reservation.

How to protect your business:

- Ensure that business accounts are protected using 2-step verification (2SV). This will help to prevent unauthorised access to your computer systems even if an attacker knows an employee's login details.
- Employees who communicate with your suppliers should be informed of what types of information a supplier will and won't ask for. For example, a supplier will never ask for an employee's password. Staff should be encouraged to speak with a supervisor if they've received a request they're unsure about.
- If you are a business, charity or other organisation which is currently suffering a live cyber attack (in progress), please call **0300 123 2040** immediately. This service is available 24 hours a day, 7 days a week.
- For more advice on how to improve your business' cyber security in an affordable and practical way, please see the National Cyber Security Centre's **Small Business Guide**

Recommended police services available to organisations in the hospitality sector:

Police CyberAlarm: is an award-winning free tool, provided by your local police force, to help your business or organisation monitor and report the suspicious cyber activity it faces. The service is made up of two parts: monitoring and vulnerability scanning. It will detect and provide regular reports of suspicious cyber activity, enabling your business or organisation to identify and take steps to minimise your vulnerabilities.

Police CyberAlarm is a monitoring system and does not interfere with normal network operations. More information about Police CyberAlarm can be accessed here: **Police CyberAlarm**

Cyber Resilience Centre (CRC): There is a police-led, not for profit Cyber Resilience Centre in every region in England and Wales to help businesses better protect themselves against cyber threats. Each CRC offers flexible membership packages to suit the needs of all businesses with the Core Membership being free of charge.

Visit your local centre’s website to discover the full range of available cyber security services: **Regional Centres - National CRC Group**

Protect network: The Protect network leads the law enforcement response of protecting the public from being targeted in a cyber-attack and empowering individuals and organisations to protect themselves. There are staff across each local police force and Regional Organised Crime Unit (ROCU) in the United Kingdom to offer consistent advice and

Cyber Essentials: This **scheme helps organisations** guard themselves against the most common cyber threats and demonstrates a commitment to cyber security. Certification gives you peace of mind that your defences will protect against the vast majority of common cyber attacks simply because these attacks are looking for targets which do not have Cyber Essentials technical controls in place. It shows you how to address the basics and prevent the most common attacks.

Recommended NCSC services available to businesses in the hospitality sector:

Early Warning service: Register (free) for the **NCSC Early Warning** (EW) service. EW is designed to help organisations defend against cyber attacks by providing timely notifications about possible incidents and security issues. The service automatically filters through trusted threat intelligence sources to offer specialised alerts for organisations so they can investigate malicious activity and take the necessary steps to protect themselves.

Board Toolkit: The **NCSC Board Toolkit** covers a range of cyber security topics, starting with an introduction to cyber security specifically written for board members. Other topics include understanding the threat, collaborating with suppliers and partners, and planning a response to a cyber incident. Each topic is filled with straightforward guidance and helpful questions that board members can ask their technical teams.

Exercise-in-a-Box: Register (free) for the **NCSC Exercise-in-a-Box**. An online tool which helps organisations find out how resilient they are to cyber attacks and practise their response in a safe environment.

CiSP: Register (free) for the **NCSC Cyber Security Information Sharing Partnership (CiSP)**. This is a secure, online forum to exchange cyber security information in real time, in a confidential and dynamic environment. Membership increases situational awareness through the sharing of threat assessments, advisories, alerts, and vulnerabilities.