IHS DAILY BUSINESS GUIDES

VISIT US AT INSIDEHS.COM

Cybersecurity: Is Your Business Doing Enough?

Why don't businesses embrace crucial security actions?

As we approach the end of Cybersecurity Awareness month, the Inside Hospitality Solutions team has reviewed this often-overlooked addition to your business security practices.

Cybersecurity is all too often seen as something we know we should do. However, sadly, a lack of knowledge, understanding and resources results in low-priority implementation. Too many businesses act or react only when a problem arises.

In this Daily Business Guide, we look at four simple steps that will immediately enhance your business's cybersecurity. We also introduce the term Quishing, a new scam your team should know to avoid security issues.

CYBERSECURITY BASICS

In the latest report on cybersecurity by Malwarebytes, it became evident that most businesses are simply failing to adopt fundamental security protection.

Ask yourself these questions:

- Do you have antivirus software installed on all your devices/networks?
- Do you utilise multi-factor authentication?
- Do you utilise a password manager?
- Do you maintain and update unique passwords?

STEP 1: PASSWORDS

Consider all the devices in your business and how you store, manage and update unique passwords.

- Do you use password manager software or
- Do you have a manual internal process?

The conundrum with passwords is that not only do they need to be unique for every device and online account, but the user wants a memorable option for easy access.

- Do you use the same password everywhere? Please say no!
- Do you mix characters, uppercase, lowercase letters, and numbers?
- Do you include children or pet names, dates of birth, wedding anniversaries and so on?
- Why would you make it so easy for the scammers out there?

STEP 2: HUMAN RESOURCES

Should an employee leave your business, have you documented a process for retrieving provided devices and accessing and changing passwords to prevent post-employment access?

We are still amazed by the frequent horror stories of an employee leaving and their critical business data being either locked out or compromised.

STEP 3: MULTIFACTOR AUTHENTICATION

Consider multi-factor authentication (MFA).

MFA is ideal for business users who struggle with password management.

Simply put, MFA is a bridge between your online accounts and the potential access to your passwords that requires a secondary ID authentication (not a password) to complete your log-in. This may be an email or SMS code message, biometric scan, or confirmation by opening a cell phone app.

Without that secondary access, even if your passwords are compromised, they cannot gain access to your accounts.

STEP 4: ANTIVIRUS SOFTWARE

Do you find antivirus software:

- Difficult to use?
- Complicated?
- In need of constant upgrades/updates, and the scammers still get through?

Many people do not fully understand what antivirus software actually does, and as a result, even if it is in place, the lowest-cost option has frequently won the day. No training has been provided on how to use it. So spend your budget wisely and ensure that training is included.

What is particularly upsetting is that sometimes, even the users of online security and privacy tools have the wrong impression about those tools.

***Top Tip:* Don't be fooled - VPN software is not designed to stop viruses or malware!**

INTRODUCING QUISHING - A TERM NOT KNOWN BY MANY

We discussed Phishing in a previous Daily Business Guide, but many people are totally unaware of Quishing.

Quishing is basically phishing using QR Codes. And the same security rules apply.

Email messages can look very convincing and include an embedded QR code or an attachment for your “easy access”. However, these codes may direct you to malware sites or those requesting your credentials.

These emails have little to no text or include an image, and they always promote the following:

- A sense of urgency or emotional temptation to act now – reducing your time to evaluate the message and sender.
- A link directing to a site requesting your personal information.

Consider:

- Is the email layout what you would expect?
- Is the email sender's address from the organisation?

If you have any concerns, do not click on the QR Code; do your research on the sender and delete the email.

Read our Phishing Daily Business Guide for further advice - https://bit.ly/IHSPhishingGuide

REQUIRE CYBERSECURITY ADVICE AND ASSISTANCE?

Looking for help? The IHS Marketing Team can support all your marketing needs, including cybersecurity, video development, website and social media audits, research and analysis, actions and activity.

Visit the www.insidehs.com/dailyupdate page for more information. Follow Inside Hospitality Solutions on LinkedIn and subscribe to our monthly newsletter.

IHS MARKETING CONTACTS

Name	Contact Information
Yuri Duncan	Yuri@insidehs.com
Marketing	+1 317 645 3824
Rich Paliwoda	Rich@insidehs.com
President	+1 917 5703827