interfuture

BUSINESS **IT** SECURITY

Interfuture Security News

April brought more challenges and opportunities in the world of cyber security: the **Interfuture Security** newsletter has the details.

Phishing continues to be the biggest threat to our clients, so we break down in detail how the user quarantine in **Outlook** works.

Additionally, we head across the pond to a story that shows the importance of training on cyber security best practise.

As always, any feedback or queries please contact us via our website or on our social media channels.

Key Point

We understand that sometimes it can be frustrating when emails are sent to quarantine when they weren't meant to - it happens to us too.

However, the inconvenience of having to manually go into the quarantine to release your email is far less than suffering a cyber attack.

Ultimately, it is better to be safe than sorry!

Quarantine Machine

We've had questions from clients about how the user quarantine in **Microsoft Defender** works. This system isolates potential phishing or spam emails before they can get to your **Outlook** inbox. Here is how it works:

1. Your admin sets up your quarantine, applying filters to best suit what you need.

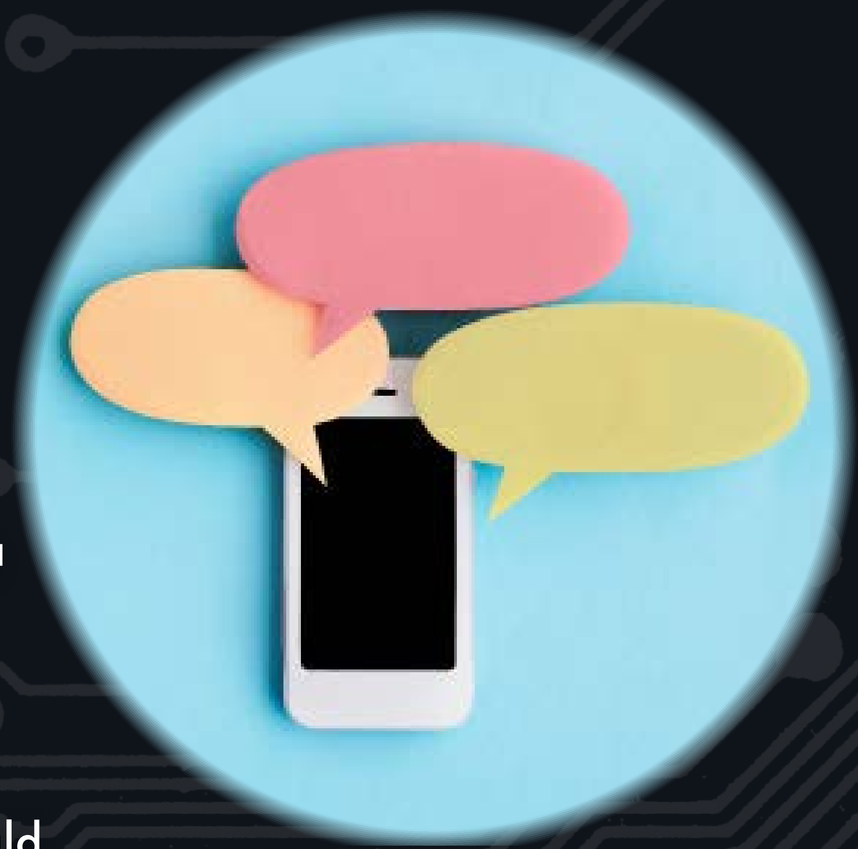
2. You receive an email in your **Outlook** inbox from support that asks you to **Review These Messages**.This contains details like the time the email was received, the date, the sender and the subject line.

3. From here you can **Block Sender** if it is spam, **Request Release** if the email is authentic, or you can **Review Message** to learn more.

4. Click on **Review Message** and you will be taken to a page on your web browser. This window will give you more information, including why the email was blocked by quarantine.

5. Close that window, select your email to **Request Release** or **Delete** the message again, or you can preview the message. Here, you can see what the message says without the content breaching your system, so if you're not 100% sure of authenticity, check here.

Mixed Signals



Late last month, I expect you heard about a group of senior officials within the US government who accidentally added a journalist to a **Signal** group chat they were using. They gave away confidential information, including the time and location of a military operation, to a member of the press.

Now, I'm not going to go into the political ramifications here – you get enough of that online, I'm sure. Instead, I wanted to think about the cyber security implications: what measures were not taken and how could the leak have been prevented.

To start with, these officials shouldn't have been talking on **Signal** in the first place. Though the app has robust features like encryption and automated message deleting, US government officials are meant to use a system in their homes that is designed to be far more secure.

Evidently, there was a lack of awareness or training: even if **Signal** held, their phones could be taken from them physically and breached. There was no verification or two-factor check to enter the chat: anyone could have been added. If a journalist managed to find their way into a high-level conversation, what is to stop someone with more malicious intent?

So, what can we (and the White House) learn from this fiasco?

1. Training your staff to be aware of cyber security is vital – even one weak link could damage an entire business (or nation!).

2. Use the right technology for the job – if you start using personal devices at work, you risk information being leaked or lost.

Could you benefit from being protected by **Interfuture Security**, who can help train your staff on best practices, as well as providing the best technology available to keep your data secure?

Friendly Competition

We wanted to set you a little challenge: someone over at our sister company **Interfuture Systems** was bragging about a new review they had received from a client - we want some reviews of our own so we can get our own back!

Every review means a lot to us - thank you.

Review Interfuture Security HERE