usecure

MSP Email Sequence

Email #1

Subject:

How quickly could a cyber criminal exploit your staff?

Email Body:

Hi [first.name],

If a cyber criminal set sights on your business today, how long do you think it would take for an employee to unknowingly compromise sensitive company information?

With human error playing a key part in over 90% of data breaches, all it takes is for one targeted phishing email to arrive in the inbox of an unwitting employee.

That's why we've launched a new service that will help your business:

- **Prevent** user-related breaches, fines and financial losses caused by human error
- **Strengthen** data loss prevention by boosting human resilience to targeted attacks
- **Demonstrate** compliance standards with key frameworks like ISO 27001

By combining regular security awareness training, periodic phishing campaigns, ongoing dark web monitoring and effective policy management, our new managed service reduces your human cyber risk by 50% in the first 12 months - without damaging productivity or draining internal resources.

Book a call with us today [insert link] to claim a free Human Risk Report (HRR) that outlines your business's current employee security posture.

usecure

MSP Email Sequence

Email #2

Subject:

What makes employees the number one cyber risk to your business?

Email Body:

Hi [first.name],

Employees are often labelled as the ‘weakest link in your cyber security chain’, but why is that?

Well, there are many reasons, but these four often stand out amongst the rest:

- **People make mistakes** - From attaching the wrong file in an email to misdirecting an email altogether, all staff make mistakes.
- **Employees don’t receive enough training** - Monthly security awareness training is proven to significantly improve security behaviour, yet some businesses still only conduct quarterly, yearly or no training at all.
- **Attacks are becoming more sophisticated** - Attackers can now purchase mountains of stolen usernames and passwords on the dark web to launch targeted attacks.
- **A lack of security policies and processes** - How often do your employees update their passwords? A lack of security policies means that employees either don’t know or don’t stick to best practices.

There are many factors your business needs to be aware of when it comes to human cyber risk - that’s why we’ve launched a free eBook on how to build a security-savvy workforce.

Download The 2022 Guide to Reducing Human Cyber Risk [insert link] today and learn how to transform employees from a security risk into a security asset.

usecure

MSP Email Sequence

Email #3

Subject:

What would you do if your staff kept getting 'phished'?

Email Body:

Hi [first.name],

What action would you take if you noticed a sudden increase in phishing emails arriving in your employees' inboxes?

For many businesses, one of the first thoughts is to flag this issue to employees and maybe share some tips on how staff can spot and report these attacks before being caught out.

Problem is, this information is quickly forgotten amongst all the day-to-day noise.

So, how can your business truly strengthen its employee security posture against evolving cyber attacks?

Through our new 'Human Risk Management (HRM)' service, you're able to understand, reduce and monitor your employees' security posture at any one time, all through:

- Ongoing security awareness training delivered in regular bite-sized sessions
- Periodic phishing simulations that track user risk against various techniques
- Ongoing dark web monitoring that identifies stolen user credentials
- Simplified policy management that tracks staff signatures and automates reminders

To celebrate our new service, we're offering a free Human Risk Report (HRR) that outlines your business's human risk score, staff phishing vulnerability as employee data is currently exposed on the dark web.

Simple fill in the form on this page [insert link] and then we'll follow up with the next steps!