

# Security Awareness Training & Phishing Simulations

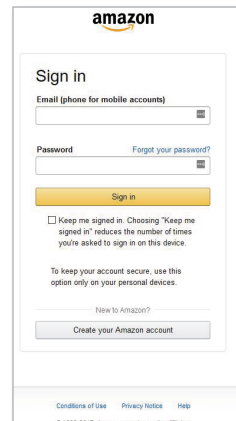
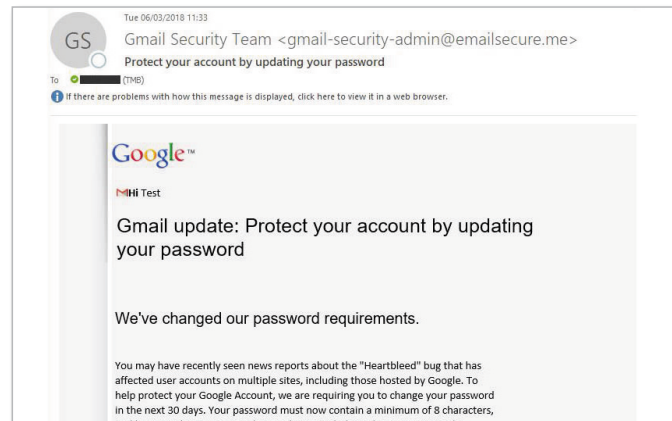


## How Does It Work?

When you sign up for TMB's phishing simulation service, we'll send a series of fake phishing emails to your organisation, spread throughout the year.

Just like real phishing emails, our fakes will try to tempt your users into clicking links or entering their contact details. But unlike the real thing, they won't cause any harm; instead, they'll point your people to helpful information and training courses, teaching them the importance of safe cyber security practices within the workplace.

## Security Awareness In Action:



## Step 1

Groups of users within your organisation will receive an email from us, which will imitate real phishing emails - right down to the mistakes that criminals often make (these act as important clues).

We might, for example, send them an invitation to claim a free Amazon voucher, or we might tell them they have a new follower on Twitter. Or we

may pretend they need to reset their login details for one of their online accounts.

There are many more tactics TMB can use, but whichever one we opt for, we'll send our fake phishing emails at random times throughout the year, so your users can't guess when they're about to be tested.



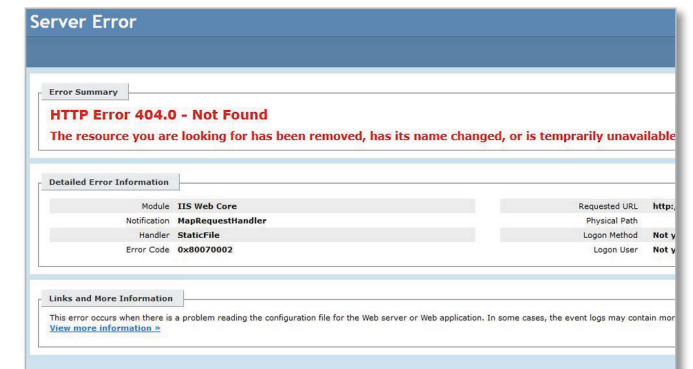
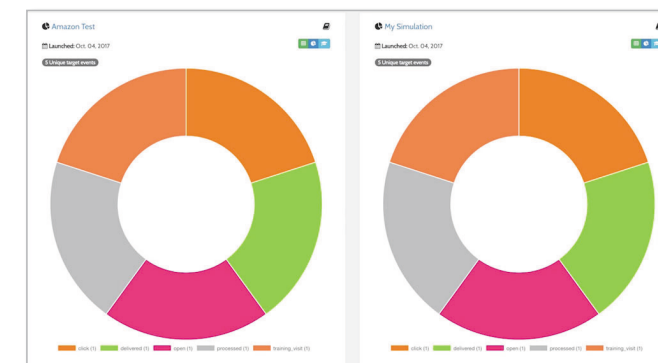
## Step 3

Any users who complete the training courses will be sent a certificate of completion, which will help you keep track of who needs training and who doesn't.

## Step 2

If a user falls for one of our fake emails, by clicking a link or entering their personal information, they'll automatically be sent to one of these:

- A training video, which informs them about the dangers of cyber crime. After this, they'll have the chance to complete a quiz, to see what they've learned.
- A ready-made landing page, with helpful cyber security information and graphics.
- A custom web page of your choice.
- A fake '404' message, which simulates a 'page not found' browser error. This is a good option if you're concerned your users might talk to each other about the fake phishing emails and give the game away.



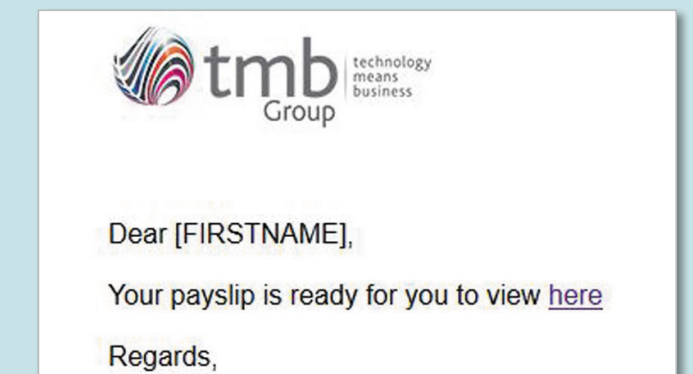
## Step 4

Once we've completed a fake phishing campaign, we'll provide a complete report of how it went. This will include general statistics, like the percentage of your organisation that fell for the trick, as well as more specific details, like which users were fooled and which ones completed the training courses.

## Bespoke Campaigns

The most dangerous form of phishing is spear-phishing, where criminals tailor their emails to your specific company and people.

To find out if your business would be susceptible to such an attack, TMB can customise our campaigns, based your company and employee details.



# What Does It Include?

## Standard Subscription

- TMB standard phishing email campaign.
- TMB standard training campaigns.
- Schedules for all activities are randomised.
- Each month will include at least one activity but may be more.
- Updating user lists in portal.

## Optional Extras (Fees Apply)

- Spear-phishing Campaign: Custom phishing emails, based on your company and employee details.
- Bespoke Training Campaign: Specific training outside of normal scheduled activities.


## Pricing


A standard 12-month subscription for TMB's Security Awareness Training & Phishing Simulations costs just £1.66 per user per month. Even better, there are absolutely no setup fees.




## Contact TMB


If you're interested in starting a subscription, please contact us for an obligation-free chat about your requirements.


 0333 900 9050

 [info@tmb.co.uk](mailto:info@tmb.co.uk)

 [www.tmb.co.uk](http://www.tmb.co.uk)

 @TmbGroup

 @TMBGroupIT

 /technology-means-business-ltd