Cybersecurity testing

Cybersecurity and the human firewall

ramsac
at the heart of IT

Table of Contents

Introduction

In this day and age, scammers are using more and more sophisticated tactics to defraud companies that they see as easy targets. Even with top-notch security systems, human error or lack of awareness can leave your business vulnerable to attack.

So it's time to test your defences, and we're here to help. We've compiled three experiments that you can run on your co-workers to help highlight some of the common ways scammers can try to take advantage of your colleagues, exposing your company to risk.

Before you begin, please remember to ensure that you have buy-in from senior management.

Test 1

Go Phish

The Experiment: Can you create a convincing email from a member of senior management to accounts, using only information from your website and social media?

For the purposes of this test, you or someone you nominate are going to create a fake email, posing as a member of your company's senior team. Firstly, you will need to identify a suitable senior team member from the website, and look for any references to them that might give away their writing style or personality, such as blog posts or company news. Using their name, create an email address on Outlook.com or a similar mainstream email provider.

While scanning the website, keep an eye out for any news that might prove useful in composing your email, such as a new big contract win or industry event.

Then, using LinkedIn, find a team member from accounts. If you can find any example email addresses on the website, use that as a template, but it is reasonable to assume that most company email addresses take common formats such as:

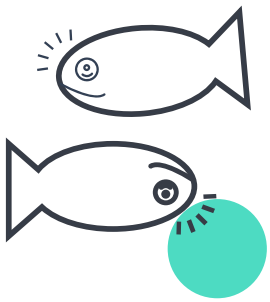
jane.smith@company.com

j.smith@company.com

jane@company.com

jsmith@company.com

Then you are ready to compose your email. Ideally, you should use a phone, so that the lack of signature is easily explained.



Example 1:

Hi Jane,

Hope you enjoyed the weekend, just a quick question. Trying to arrange an event for BIG NEW CLIENT/SENIOR TEAM MEMBER, and we need to transfer a deposit to the venue. Can you let me know what details you need to authorise payment?

Good if we could sort today.

Thanks,

John

Sent from my iPhone

Example 2:

Hi Jane,

Hope you're well, just a quick request. I've been speaking to Mark at BIG SUPPLIER, and he's asking how quickly we can update account details as they've changed banks?

SORT CODE: 00-00-00
Account Number: 00000000

Would be great if we can sort this quickly, especially with BIG NEW CLIENT on the horizon.

Thanks,

John

Sent from my iPhone

Ideally, you'll be met with: scepticism; a request for a call or a face-to-face meeting; or even silence. In the (hopefully) unlikely event that you are successful, inform your colleagues immediately.

Test 2

Calling Time

The Experiment: Can you convince someone to compromise security information in the time it takes to make a short phone call?

For the purposes of this test, you or someone you nominate are going to pose as someone from Human Resources or IT. You will contact company employees in an attempt to get them to compromise their security information.

Using an external phone, call in to reception and ask to be put through to someone named on the website or who you've found on LinkedIn, ideally from HR, IT or Accounts/Finance. If you're asked what it is regarding give a generic name (but not too generic!) and say that it's a routine call.

Here's an example of the kind of script you might want to use for this experiment:

Caller: Hi there (Employee), I'm calling from (HR or IT). We're in the process of updating our records for support staff. Can you please tell me your current password and username combination?

Employee: Sorry, what is this for?

Ca: Oh sorry, it's for logging in to your computer. So, your username is?

Employee: joe.bloggs

Ca: And the password?

Employee: Jenny11Sam7

Ca: Ok, great. Do you use that password for any other systems?

Employee: Yes, I use it for the accounts platform.

Ca: Right, is it the same username?

Employee: No, that one is j.bloggs1

Ca: Thank you for your help, would you mind putting me through to one of your colleagues?

Test 3

Shut the front door

The Experiment: Can someone get into your office without being held up by security?

Last but by no means least, this challenge will be the hardest to put together. For the purposes of this test, you'll need a person who your colleagues would not recognise to attempt to bypass security and enter your company's building.

At ID or employee pass doors, you can use one of two tactics:

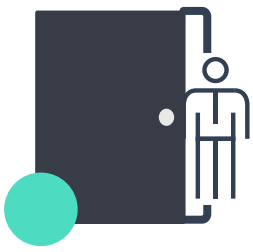
- Follow someone in at a busy time such as quarter to nine or lunchtime.
- Wait for someone to be coming out.

If you have to pass reception, try to avoid eye contact and look as if you know where you're going. If you're asked to sign in or if you have an appointment, give a generic name, and say you're visiting a particular person who you've found on LinkedIn. If they offer to call them, say: "It's fine, I know how to find them."

At code doors, the two tactics to try are:

- Pretending to have forgotten the code and being apologetic.
- Carrying something awkward or seemingly heavy, so people feel obliged to help you.

This test may not pose the biggest risk to your business, especially if you do not handle cash in your office. But it can be a serious concern if your colleagues leave items such as mobile phones on their desks, or if company computers and laptops are left unsupervised.



Report on findings

Once you've completed your experiments, it's time to reflect on what you've uncovered. Even if all of the tests failed, you may have exposed other vulnerabilities that need addressing, such as a need for better screening of calls and visitors coming in to reception.

Ensuring that cybersecurity awareness levels are high in your organisation is one of the most important tools you have to protect your business from fraud. Even if you are completely satisfied with your results, it may be worth holding a briefing with your

Find out more

As well as providing advice and configuration for the physical security of IT data, ramsac also offers an innovative online staff training programme which can be used to help develop your human firewall protection and awareness. If you'd like to find out more, why not get in touch.

Call: **01483 412 040**

Email: **info@ramsac.com**

Visit: **www.ramsac.com**

ramsac
at the heart of IT

ramsac limited
Godalming Business Centre
Woolsack Way
Godalming, Surrey
GU7 1XW

www.ramsac.com
01483 412 040