Overview

The Employee Cybersecurity Challenge Guide is designed for companies who are ready to take a more engaging and immersive approach to reinforcing the cybersecurity awareness, knowledge and measures of employees. It is a flexible, plug-and-play guide.

The Challenge will gamify common cyber threats at the workplace, in order to encourage employees to recall and perform the cybersecurity measures they have learned through the preceding Kit assets. The company will also be able to evaluate the state of cyber-readiness of the company and keep track of which of the simulated cyber threats they might need to step up on protecting against.

The challenge consists of setting up three basic cyber threats and sending them out to employees. These cyber threats are:

1. Phishing e-mails
2. Privacy breach
3. Unsecured WiFi networks

It is recommended that this challenge take place over three to four weeks, depending on the company's resourcing capability. Companies can choose which challenges they wish to carry out and the sequence in which to carry them out.

1. Plan

1. Rope in stakeholders

2. Plan roll-out
- Select challenges and sequence
- Appoint leads for each challenge
- Set timeline

2. Execute

1. Announce the start via e-mail

2. Execute the Phishing E-mail Challenge
- Set up a phishing e-mail address
- Set up a webpage
- Set up a Google Analytics account
- Set up and send phishing e-mail

3. Execute the Privacy Breach Challenge
- Set up a phishing e-mail address
- Set up a Google Form
- Set up and send phishing e-mail
- Send notification e-mail

4. Execute the Unsecured WiFi Challenge
- Identify suitable location(s)
- Set up equipment and network
- Monitor and track
- Set up and send notification e-mail

3. Conclude

1. Set up a feedback form

2. Announce the end via e-mail with feedback form link

1. Plan

1.1. ROPE IN ALL NECESSARY STAKEHOLDERS

- **You will need support from several departments to plan and coordinate this:** Ensure that management, the HR and IT departments are present for the planning, and are aligned on the objectives and expectations of this Employee Cybersecurity Challenge.
- **You might need additional support to execute this:** Consider roping in some of your Employee Cybersecurity Advocates to help execute this challenge.

1.2. PLAN THE ROLL-OUT

- **Select your challenges and plan your timeline:** Based on your company's technical capability and resource availability, decide which of the cyber threats in the next section the planning committee wishes to carry out, in which sequence and a suitable time period for execution, by laying out a roll-out timeline from preparation to execution to wrap-up. The recommended duration for set-up is a week, and subsequently, the release of one challenge per week.
- **Appoint leads for each stage**: Decide who will lead the announcements of the beginning and ending of the challenge, each of the challenges you wish to carry out and tracking the outcomes of all the challenges. It is recommended to appoint one individual for each of these stages.

2. Execute

2.1. ANNOUNCE THE START VIA E-MAIL

- Notify employees so that they do not feel as if they have been caught off-guard and to mitigate possible negativity about being automatically included in the challenge when it is launched.
- Below is a suggested template for the e-mail that you may choose to adapt for use:

Hi [Name],

As you know, we take cybersecurity very seriously at [company's name]. As part of our ongoing Employee Cybersecurity Programme, we have designed

an immersive game to reinforce the cybersecurity measures you have been learning about the past few weeks. This game will take place over [duration].

From [start date] to [end date], we will be simulating three cyber threats at the workplace. Think of it as the computer game version of a fire drill!

Don't worry if you do not manage to pass these challenges. This is meant to be a fun learning opportunity. The system will automatically notify you if there are areas you need to improve on. The Employee Cybersecurity Committee will only be able to see which threat appears to be the most pressing for us as a company to guard against.

May the odds be ever in your favour!

Best regards,

[Your name and designation]

2.2. EXECUTE THE CHALLENGES

2.2.1. The Phishing E-mail Challenge

This challenge involves sending out to employees a phishing e-mail to convince them to click on a suspicious link within.

Phishing e-mails are one of the most common cyber scams used by cyber criminals to trick people into downloading malware into their devices or connected networks. It is a common cyber threat that businesses face today, and one that spam/junk filters alone cannot fully protect employees against.

The phishing e-mail that you are going to be sending out will be about a billing problem related to compensation of corporate expense claims. These e-mails typically appear to be sent by banks or the company's finance department to notify the employee that there has been a problem in reimbursing the employee's expense

claims. The employee is requested to go to a website to verify their bank account details in order to complete reimbursement.

2.2.1.1. Set up an e-mail address.

This is the e-mail address from which you will be sending the phishing e-mail. There are two ways in which you can set this e-mail address up, depending on the IT department's allowances:

1. Create a new e-mail address under your company's domain

   As this e-mail is supposed to originate from the bank your company uses or your company, it is recommended to use an e-mail address that looks similar but not identical to that which your finance department frequently uses. For example, if your finance department frequently uses 'finance@[companydomain].com', the phishing e-mail address could be 'financedept@[companydomain].com'.

   The phishing e-mail address could also contain finance-related legitimate-sounding words. Suggestions include:

   - expenses@[companydomain].com
   - reimbursement@[companydomain].com
   - paymentadvice@[companydomain].com

   Remember to set your name as "[Company name] Finance".

2. Create a new e-mail address on a free-to-use platform

   If you are unable to create an e-mail address under your company's domain, creating one on a free-to-use platform such as Gmail, Yahoo or Hotmail will also suffice. Gmail is recommended as the Gmail account can be used to set up a Google Analytics account to help track who has clicked on your link (*please refer to following section*).

   Sending a phishing e-mail address from a free-to-use platform will only serve as another indicator that this e-mail may not be legitimate. It is recommended to include your company's name and a finance-related word in the e-mail address. Suggestions include:

- [Company name]finance@gmail.com
- [Company name]advising@yahoo.com
- [Company name]expenses@hotmail.com

Remember to set your name as "[Company name] Finance".

2.2.1.2. Set up a webpage.

A webpage must be set up so that a link may be placed within the phishing e-mail, on which employees are encouraged to click to 'verify their bank account details'. This webpage will showcase a message from the company announcing the phishing e-mail as the first challenge in the Employee Cybersecurity Challenge, along with tips to recognise phishing e-mails.

A simple webpage can be set up using any one of your company's internal platforms, or free-to-use platforms. Recommendations include:

- A page on your company's intranet platform or website
- A post or tab on your company's Facebook Page
- A document on Google Drive, Microsite OneDrive, Box.com or Dropbox, of which the link is accessible to but not editable by all who have the link

It is recommended that the URL of the webpage be shortened using Google URL Shortener or Bit.Ly Link Shortener, so that employees may not see the actual URL when they hover over the link, and you can track how many people actually clicked on the link.

Below is a message template that you may wish to adapt for use:

> Hello!
>
> That was the first challenge in our Employee Cybersecurity Challenge! The link that you have just clicked on is a phishing link, and could have caused malware or worms to be downloaded into the company's networks and systems.

Phishing e-mails are commonly used by hackers to lure recipients into downloading malware/worms into your devices, and any other devices your devices may then be connected to. These malware may then corrupt your files and systems or steal confidential information from them.

Phishing e-mails and links often look legitimate, but they also almost always contain signs that indicate otherwise. Did you notice that there were grammatical errors in the e-mail? Check the e-mail for other signs you might have missed. Most importantly, stop and think before clicking on suspicious emails!

Your awareness and actions can help protect the company. Thank you.

Cheers,

[Your name & designation]

2.2.1.3. Set up a Google Analytics account

In order to track which employees opened your phishing e-mail and clicked on the link, a free solution like Google Analytics (GA) would suffice. While GA is traditionally used to track and report a website's traffic and consumer engagement, it can also be used to track email activity.

- In order to get the GA tracking system in place to monitor the employees' phishing alertness, sign-up for a Gmail account and create your GA account here.
- Once the account has been created, follow the instructions to set up your Tracking ID here.
- Event tracking is done via the embedding of an image tag within the HTML code of your phishing email. Detailed instructions of how to use Event Tracking within GA are available here.

- The URL of the image contains all the information necessary for GA to track the emails being sent out and more important, which employee has click and opened it.
- Some the guides below are recommended for reference in setting up the backend tracking:
  - How To Track Email Opens with Google Analytics (Mike Veilleux, 2014)
  - Email campaign tracking with Google Analytics (Dave Chaffey, 2014)
  - How To Track Email Campaigns In Google Analytics (Oliver Raymer, 2014)

2.2.1.4. Set up and send out phishing e-mail

Phishing e-mails may look legitimate at first glance, but they often contain small signs that indicate it might not come from a legitimate sender, such as an unofficial e-mail address, poor spelling and grammar, generic greeting style such as 'Hi', 'Dear Employee' or 'Dear Customer', and the inclusion of links which the recipient is encouraged to click on.

Below is a suggested template for the e-mail that you may choose to adapt for use:

E-mail subject: Expenses Claims Payment Advice

Dear Sir/Madam,

This e-mail has been issued at the request of our customers. We have detected a billing problem with regards to the reimbursement of your expense claim, dated last month.

Kindly verify your bank account detail at [URL of the webpage you have set up] so that we may proceed with payment.

Yours fatefully,

Global Payments and Cash Management

[Name of bank company uses]

***

Security tips

1. Install virus detection software and personal firewall on your computer. Updates software regularly to ensure you have the latest protection.

2. To prevent viruse or other unwanted problems, do not open attachments from unknown or non-trustworthy sources.

3. If you discover any unusual activity, please contact us as soon as possible.

***

2.2.2. The Privacy Breach Challenge

Aside from tricking people into downloading malware into their devices or connected networks, phishing e-mails are also used to convince people to give away confidential information.

This challenge involves sending out of a phishing e-mail to convince employees to not just click on a link this time, but also input their details on a website designed to look legitimate. Its aim is to check how many employees unwittingly give away personal information that could possibly be used against the company.

The phishing e-mail that you are going to be sending out for this challenge will alert employees of attempts to log into their corporate account. These e-mails should appear to be sent by one of the company's service providers or the company's IT department, alerting the employee that several log-in attempt errors were observed for the employee's corporate account. The e-mails then instruct the employee to go to a link to verify their corporate account details before the supposed service provider or IT department suspends the corporate account. The e-mail should redirect employees to a website where they are encouraged to enter confidential information.

2.2.2.1. Set up an e-mail address

This is the e-mail address from which you will be sending the phishing e-mail. There are two ways in which you can set this e-mail address up, depending on the IT department's allowances:

1. Create a new e-mail address under your company's domain

   As this e-mail is supposed to originate from the company's IT service provider or your company's IT department, it is recommended to use an e-mail address that looks similar but not identical to that which your IT department frequently uses. For example, if your IT department frequently uses 'IT@[companydomain].com', the phishing e-mail address could be 'ITdept@[companydomain].com'.

   The phishing e-mail address could also contain IT-related legitimate-sounding words. Suggestions include:

   - ITHelp@[companydomain].com
   - ITverification@[companydomain].com

- ITalert@[companydomain].com

Remember to set your name as "[Company name] IT".

2. Create a new e-mail address on a free-to-use platform

   If you are unable to create an e-mail address under your company's domain, creating one on a free-to-use platform such as Gmail, Yahoo or Hotmail will also suffice. Gmail is recommended as the Gmail account can be used to set up the Google Form in which employees will be asked to input their 'verification details' (*please see next section*).

   Sending a phishing e-mail address from a free-to-use platform will only serve as another indicator that this e-mail may not be legitimate. It is recommended to include your company's name and an IT-related word in the e-mail address. Suggestions include:

   - [Company name]IT@gmail.com
   - [Company name]ITsupport@yahoo.com
   - [Company name]ITalert@hotmail.com
   - [IT service provider name]IT@gmail.com

   Remember to set your name as "[Company/IT service provider name] IT".

2.2.2.2. Set up a Google Form

The objective of this challenge is not to have employees give away actual confidential information, but to see if they might be misled into doing so. It is recommended that the form only require the employees to key in details which the company is comfortable with employees giving out. The minimum detail required would be the employee's full name.

- Create the form here.
- Title your form '*Verify account details*' and insert in the form description '*Several log-in attempt errors were observed for your corporate account. Please input the required details below to verify that you are the legitimate owner of this account*'.

- Select the question type to be 'Text', with the title 'Full Name'. Make it a required question by checking the box next to 'Required question'.
- You may wish to duplicate the above if you would like your employees to input more details, such as their corporate e-mail address and/or contact details.
- When you are done, click on 'File' on the top bar and save the Form.
- Click on 'Send form' on the top right-hand corner. Under 'Link to Share', check the box next to 'Short URL' and copy the URL that appears in the field above. This is the URL to include in your phishing e-mail.
- For back-end tracking of your Form results, click on 'Responses' on the top bar and go to 'View responses'. This will bring you to a Google spreadsheet where all responses by employees will be captured. You should be able to see the names of the employees who willingly gave away their details.

2.2.2.3. Set up and send phishing e-mail

Phishing e-mails may look legitimate at first glance, but they often contain small signs that indicate it might not come from a legitimate sender, such as an unofficial e-mail address, poor spelling and grammar, generic greeting style such as 'Hi', 'Dear Employee' or 'Dear Customer', and the inclusion of links which the recipient is encouraged to click on.

Below is a suggested template for the e-mail that you may choose to adapt for use:

E-mail subject: Verify your account details

Dear employee,

We are writing to inform you that several log-in attempts were observed for your corporate account. Please do not be alarmed. For security purposes, we will be temporarily suspending your account until you verify your details here [embed URL of the Google Form].

We apologise for the inconvenience and appreciate your understanding.

Best regards,

[IT department of company] OR [IT service provider]

2.2.2.4. Send notification e-mail

Over the course of a week, monitor the Google Form Responses Spreadsheet to see how many employees have willingly given away their details. Once the responses have completely stopped coming in, send an e-mail to employees who willingly gave away their details to notify them and give them tips in recognising phishing e-mails. Below is a template you may wish to adapt for use:

Dear [employee name],

That was the second challenge in our Employee Cybersecurity Challenge! The details which you shared in the link embedded within the e-mail could have been used against you and the company by hackers.

Phishing e-mails are commonly used by hackers to lure recipients into giving away confidential information, so that they may use these details to infiltrate company networks.

Phishing e-mails and links often look legitimate, but they also almost always contain signs that indicate otherwise. Did you notice that the e-mail did not directly address by your name and that the URL was not hosted on the company's server? Check the e-mail for other signs you might have missed. Most importantly, stop and think before clicking on links in suspicious emails!

Your awareness and actions can help protect the company. Thank you.

Cheers,

[Your name & designation]

2.2.3. The Unsecured WiFi Challenge

WiFi is a common part of our lives these days. We rely on it at work when we need to move around the office, and we sometimes use it to work on the go. However, many employees still do not know how to check if the WiFi networks they use are secured and safe enough to send confidential work information on, and hackers are able to use such unencrypted and unsecured WiFi networks to snoop on information being sent across these networks or to hack into the devices connected to these networks.

This challenge involves the setting up of an unsecured WiFi hotspot within the office. Its aim is to test if employees are able to recognise when a WiFi network is unsecured or will choose to use an unsecured WiFi network without considering the consequences.

2.2.3.1. Identify suitable location(s).

You may choose to identify more to place additional WiFi hotspots if you wish to. Ideal locations include places where:

- Existing access points (AP) can be easily switched off without disrupting the rest of the organisation.
- Employees are required to use the office's WiFi network instead of Ethernet cable connections.
- Employees frequently gather to do non-crucial work, such as have face-to-face meetings or social activities, such as rooms for internal meetings or the pantry.

2.2.3.2. Set up equipment and network.

There are two options for the implementation depending on your preference and capabilities:

Option 1:

- Configure a separate router, which ideally should be an enterprise router, to set up the alternative AP.
- This router will tap on the existing Internet infrastructure within the office.

Option 2:

- Utilise a 3G/4G WiFi dongle connected to a laptop for Internet access.
- The laptop will act as the WiFi router, monitoring all the incoming and outgoing web traffic.
- This set-up will keep the Internet utilisation separate from the office's ISP.

The unsecured WiFi hotspot should be named similarly to the company's network. For example, if the company AP name is "CompanyWiFi", the unsecured AP name could be "CompanyWiFi1". This WiFi hotspot should not require any log-in details.

Before switching on the unsecured WiFi hotspot, switch off the official AP at the identified locations for the challenge duration. This will cause employees' devices to prompt them to connect to a new WiFi network.

2.2.3.3. Monitor and keep track of the situation.

Employee Cybersecurity Advocates could be situated near the identified locations to observe how many employees actually logged onto the unsecured network.

It is also recommended to set up the backend router management for tracking the number of employees who have logged onto the unsecured WiFi network. Backend router management should be able to keep track of the following:

- Number of employees who logged onto the alternate network to surf the internet
- Details (specifically device name) of the employee who have logged on.

2.2.3.4. Set up and send notification e-mail to all those who have accessed the unsecured WiFi.

Once you have collected the names of all employees who connected to the unsecured WiFi network, it is recommended that you follow up with an email to them at the end of the challenge, explaining to them the consequences of logging onto an unsecured WiFi network.

Below is a template you may choose to adapt for use:

> Hi [name],

The new WiFi network you connected to today is the final part of the Employee Cybersecurity Challenge! The WiFi network was unsecured, and the information that you were sharing over the network could have easily been snooped on by hackers.

Unsecured WiFi networks not only allow hackers to see what you are doing on your devices connected to the networks, they also allow hackers to access all the information on your devices and infiltrate the systems and other networks your devices might be connected to, such as the company's shared servers.

Did you notice that the WiFi network did not require log-in details? You can also check the name of the WiFi network as it will usually attempt to look similar to legitimate networks with one or two slight errors. Most importantly, stop and think before connecting to new WiFi networks! If it is not absolutely urgent, consider waiting till you can connect to a secured WiFi network.

Your awareness and actions can help protect the company. Thank you.

Cheers,

[name & designation]

3. Conclude

3.1. SET UP A FEEDBACK FORM

- **It is important to gather feedback from employees on their experience:** Set up a survey on a free-to-use platform, such as Google Forms.
- **Keep the feedback form short:** This will make it easier for employees to complete and minimise the amount of data you have to sift through. The following 3 questions are recommended to be asked:
  a. What have you learned from this challenge?
  b. How did you feel about this experience?

c. Would you look forward to more of such forms of engagement on cybersecurity, or even other important company matters, in the future? Tell us why.

3.2. ANNOUNCE THE END VIA E-MAIL

- **Conclude the end of the Employee Cybersecurity Challenge**: Employees are aware that you have been carrying out the Challenge and they will appreciate knowing when it has come to a close.
- **Insert the feedback form link into the e-mail:** This is to ensure that employees know that there is an outlet through which they can communicate their thoughts and concerns.
- **Share generic findings from the challenge**: It is important to close the challenge with some results so that employees know that there is follow-through and next steps. The type of findings you should be sharing depends on how well your employees have fared, which can be extrapolated into two scenarios:
  a. Scenario 1 – Employees do well with less than 30% of them falling for all challenges
     - Send an e-mail to praise the employees on a job well done and to keep up their cybersecurity. You may choose to adapt the template below:

> Hi all,
>
> Thank you for taking part in the Employee Cybersecurity Challenge! We're proud to share that less than 30% of you fell for the cyber threats we simulated and it's an encouraging sign that we are well-prepared for the many cyber threats that companies face out there today.
>
> While we fared well, there's still much we can improve on, so don't forget to check out the posters we have put up around the office, keep up-to-date with cybersecurity news, and talk to your Employee Cybersecurity Advocate colleagues if you have any questions or concerns!
>
> If you have any feedback to share, you may do so at [URL of the feedback form]. We'd love to hear from you.
>
> Your awareness and actions help keep the company safe.
>
> Cheers,

[name and designation]

b. Scenario B – Employees do not do very well, with more than 60% of them falling for one or more challenge(s)

- Send an e-mail to thank employees for participating while highlighting that as a company, much can be learnt from this challenge. Highlight the continuous need for employees to stay updated on cybersecurity news and knowledge and to practice good cybersecurity measures to keep themselves, their colleagues and their company protected. You may choose to adapt the template below:

Hi all,

Thank you for taking part in the Employee Cybersecurity Challenge! This Challenge has highlighted to us where there is much to be improved on when it comes to our day-to-day online habits, especially when it comes to [insert the challenge which the most number of employees did not pass].

When in doubt, always check with the IT department or Employee Cybersecurity Advocate colleagues, or contact the sender of the e-mail directly. Don't forget to check out the posters we have put up around the office and keep up-to-date with cybersecurity news!

If you have any feedback to share, you may do so at [URL of the feedback form]. We'd love to hear from you.

Your awareness and actions help keep the company safe.

Cheers,
[Your name and designation]

Tips for the Challenge

- Ensure that the necessary security measures are in place for each of the challenges.
- Consider keeping track of the number of employees who do not pass each of the challenges. This way, vulnerable employees can be identified for further cybersecurity training. Another suggestion would be to follow up with them one-on-one to help them understand why they did not pass so that this can become a learning opportunity for them.
- Do not create a wall of shame. Do not publicly reveal the name of employees who did not pass the challenges.
- Considering setting aside small rewards for those who passed all three challenges, to encourage them to continue practising cybersecurity. These could include little snacks, office stationery or even office memorabilia.