Reducing the risks around phishing: strategy worksheet

Looking to refresh or revisit your strategy, approach and tactics to reduce phishing? Use this worksheet to kickstart your planning or to enable conversations with the right people.

Note that this worksheet isn't designed to be a comprehensive checklist to reduce phishing, but an aide to get your thinking.

What are the top five apps, channels and technologies within your organization where phishing attacks are possible?

1.	
2.	
3.	
4.	
5.	

Are there any additional unauthorized apps or channels ("shadow IT") used on work devices where phishing attacks are possible?

1.	
2.	
3.	

Are there any opportunities to consolidate channels or use alternative tools to reduce the chances of phishing?

What IT security policies are in place or should be in place to reduce the chance of phishing, or limit the damage caused by phishing?

	Policy	**Is it currently in place?**	**If yes, how well is it enforced?**
1.			
2.			
3.			
4.			
5.			

Do you have a system or process for reporting phishing attacks? If so, how effective is it and how well is it adopted?

Name three ways that employees are currently made aware of phishing attacks and their danger.

1.	
2.	
3.	

Think of three additional or improved ways that you could spread awareness about phishing.

1.	
2.	
3.	

What anti-phishing solutions (including monitoring software etc.) do you have in place that can help reduce phishing and its impact?

1.	
2.	
3.	
4.	
5.	

Are there any additional solutions that could help?

How do you currently measure / report on the success of anti-phishing initiatives? Are there improvements you could make?

Considering all of the above think of five priority actions or next steps that will tangibly improve your approach to reducing phishing.

	Priority action	Who’s involved?
1.		
2.		
3.		
4.		
5.		

Need help? Check out an example worksheet on the next page

EXAMPLE

What are the top five apps, channels and technologies within your organization where Phishing attacks are possible?

1.	Email / Outlook
2.	SMS
3.	Microsoft Teams – chat etc.
4.	Internet browser (Chrome, Edge)
5.	Telephone scams

Are there any additional unauthorized apps or channels ("shadow IT") used on work devices where phishing attacks are possible?

1.	WhatsApp (Mobile)
2.	Social media (Facebook, Snapchat etc.)
3.	Private email (e.g. Google Mail etc.)

Are there any opportunities to consolidate channels or use alternative tools to reduce the chances of phishing?

Use secure intranet software for news items to reduce emails; use chat on intranet software as a "WhatsApp" killer.

What IT security policies are in place or should be in place to reduce the chance of phishing, or limit the damage caused by phishing?

	Policy	**Is it currently in place?**	**If yes, how well is it enforced?**
1.	Two factor authentication where possible	Yes	Well enforced
2.	Zero trust policy for access	Yes	On core systems only
3.	Cybersecurity check list for new procuring new software	Yes	Well enforced
4.	90 days force password reset	Yes	Where possible
5.	Company owned devices only for network access	No	Not yet introduced

Do you have a system or process for reporting phishing attacks? If so, how effective is it and how well is it adopted?

One click via Outlook to report suspected phishing email is hard to find so there is low adoption. Not available on mobile devices. New extra phishing email box has low awareness.

Name three ways that employees are currently made aware of phishing attacks and their danger.

1.	Cybersecurity hub on the intranet – lots of anti-phishing material
2.	Annual mandatory cybersecurity training – anti-phishing module
3.	Externally provided phishing training where users have to spot phishing emails

Think of three additional or improved ways that you could spread awareness about phishing.

1.	**Introduce local cybersecurity champions network to drive anti-phishing awareness across each location**
2.	Create an anti-phishing round-up / update newsletter or story and publish on the intranet
3.	Create series of bitesize anti-phishing videos – including new threats from AI

What anti-phishing solutions (including monitoring software etc.) do you have in place that can help reduce phishing and its impact?

1.	Microsoft 365 / Microsoft Teams settings
2.	Cloud email security product
3.	Anti-virus software
4.	Mobile device management solution
5.	Various monitoring tools

Are there any additional solutions that could help?

Possibly. We plan to review monitoring and protection tools

How do you currently measure / report on the success of anti-phishing initiatives? Are there improvements you could make?

Threats identified and blocked through anti-phishing software; % identification rate by employees of fake phishing emails sent by training provider; number of phishing emails reported; user views of anti-phishing resources. We could add metric relating to how quickly a phishing email is reported. Also publish the report on the cybersecurity hub on the intranet.

Considering all of the above think of five priority actions or next steps that will tangibly improve your approach to reducing phishing.

	Priority action	Who's involved?
1.	Run campaign to recruit cybersecurity champions	IT, Comms, HR
2.	Use intranet news and chat function to reduce channels	IT, Comms
3.	Create new monthly update for the intranet and incorporate key stats and also the first one-minute video (Who's going to star in it?)	IT, Comms
4.	Review the design of the report phishing button in Outlook to make it more prominent. Create an additional phishing reporting form with workflow on the intranet.	IT, Comms
5.	Carry out anti-phishing tool review and make recommendations	IT