TO CLICK OR NOT TO CLICK

What we Learned from Phishing 80,000 People

F-Secure

CONTENTS

KEY FINDINGS

Staff employed in IT related roles are no less susceptible to phishing than the rest of the organization.

The number of suspicious emails that are reported is directly influenced by the process of reporting an email.

Speed is critical for all parties in an attack.

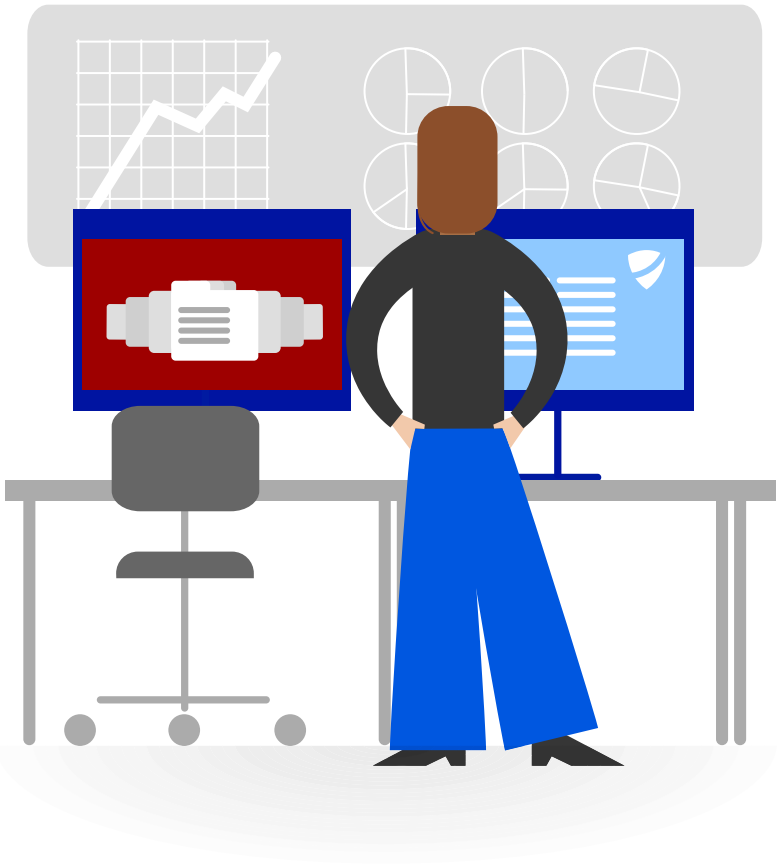
EXECUTIVE SUMMARY

F-Secure conducted a large-scale email phishing study, seeking to explore why phishing continues to be the paramount access method of malicious cyber actors. 82,402 individuals participated in the study, made up of staff from four organizations. We believe this study to be the largest so far to explore which tactics are most effective in driving clicks on phishing emails.

Each individual was randomly allocated to receive one of four simulated phishing emails (page 6 - 9). The four emails used as part of the study represented four of the most common phishing tactics: CEO Fraud, Internal HR Mimic, Document Share, and Service Issue Notification. The first objective of the study was to explore which phishing tactics are most effective in driving clicks. The second objective was to understand how other factors such as time pressure, familiarity with software, and departmental role may affect clicks.

If the individual clicked on the link, they were taken to a web page informing them that the email was part of a simulation and provided a short survey that explored some of these factors. Those individuals that filled out the survey were provided with point in time training, explaining how to identify malicious emails in the future.

Internal HR Mimic was clearly the most effective phishing email type with 4,520 of the 20,061 targeted clicking on links in the email. CEO Fraud was also effective, but less so. Document Share and Service Issue Notification both elicited some clicks, but from fewer than the other two email designs. In terms of reporting, all emails except Internal HR Mimic elicited more reports than clicks. In a real attack an efficient security team may be able to take protective actions because of these reports.



STUDY DESIGN AND METHODOLOGY

F-Secure wanted to better understand what types of phishing attack are most effective and who might be most at risk from them. We designed a study to test the efficacy of realistic phishing emails with a large number of individuals from several organizations. Our goal was to gain a comprehensive understanding of the multiple driving forces behind phishing susceptibility.

Participants

As we were seeking to explore susceptibility in a structural context, we approached a variety of organizations to participate. Those that signed up provided consent for their staff to be tested and their clicks to be recorded. Consent for participation was provided by the employer in each organization, while participation in the follow-up survey was entirely voluntary.

The organizations that participated will remain anonymous. However, their industry sectors include banking and finance, retail, and manufacturing.

82,402 individuals from four organizations were sent one of the four emails. Whether they clicked, the dates, times, their department, and country were recorded. The emails were drip-fed over a week, with all campaigns conducted between January and March 2021.

Emails

The study used four emails. Each individual received only one of these emails, which was selected at random. The emails used were chosen as they represented the most common phishing email attacks targeted at organizations. To avoid unwanted variation between the results of each organization we did not mimic real brands or organizations in the emails themselves. For example, if we had mimicked a Microsoft SharePoint shared file, we should expect a higher click rate in the organization that uses SharePoint versus those that use Google Drive etc. For operational reasons we had to make certain concessions when designing the emails to use. For details please see ‘Study Choices’ in the appendix.

Screenshots of the emails and a brief description follow.

Survey questions

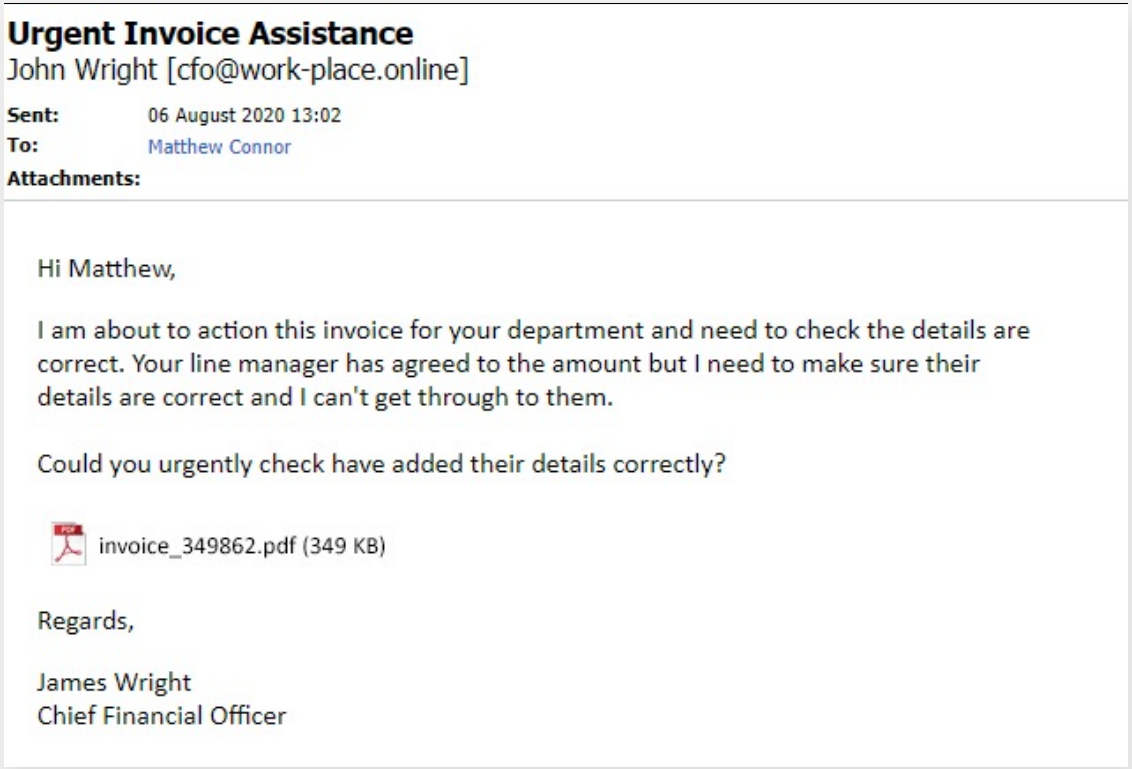
The individuals who clicked on any of the links in the emails were immediately presented with a web page informing them the email was a simulation and asking them to fill in a short survey. The survey recorded information about their use of the internet, experience with phishing emails in the past, and most recent anti-phishing awareness training.

CEO Fraud

This style of attack is sometimes called Business Email Compromise (BEC) and has been responsible for the loss of very large sums of money since it came into use. It is noteworthy because the attacker is often not seeking to deliver malicious code, or steal credentials with the email. Rather, they are seeking to convince the recipient to transfer money to an account owned by them. This type of email is often targeted towards those within the business who control finances and would likely be made to look like it came from someone senior within the business itself.

In this email we tweaked the design so it is applicable to all recipients, rather than just those who deal with finances. We also added a link disguised as an attachment to measure susceptibility by a click.

Figure 1: Sample CEO Fraud Email



Urgent Invoice Assistance
John Wright [cfo@work-place.online]

Sent: 06 August 2020 13:02
To: Matthew Connor
Attachments:

Hi Matthew,

I am about to action this invoice for your department and need to check the details are correct. Your line manager has agreed to the amount but I need to make sure their details are correct and I can't get through to them.

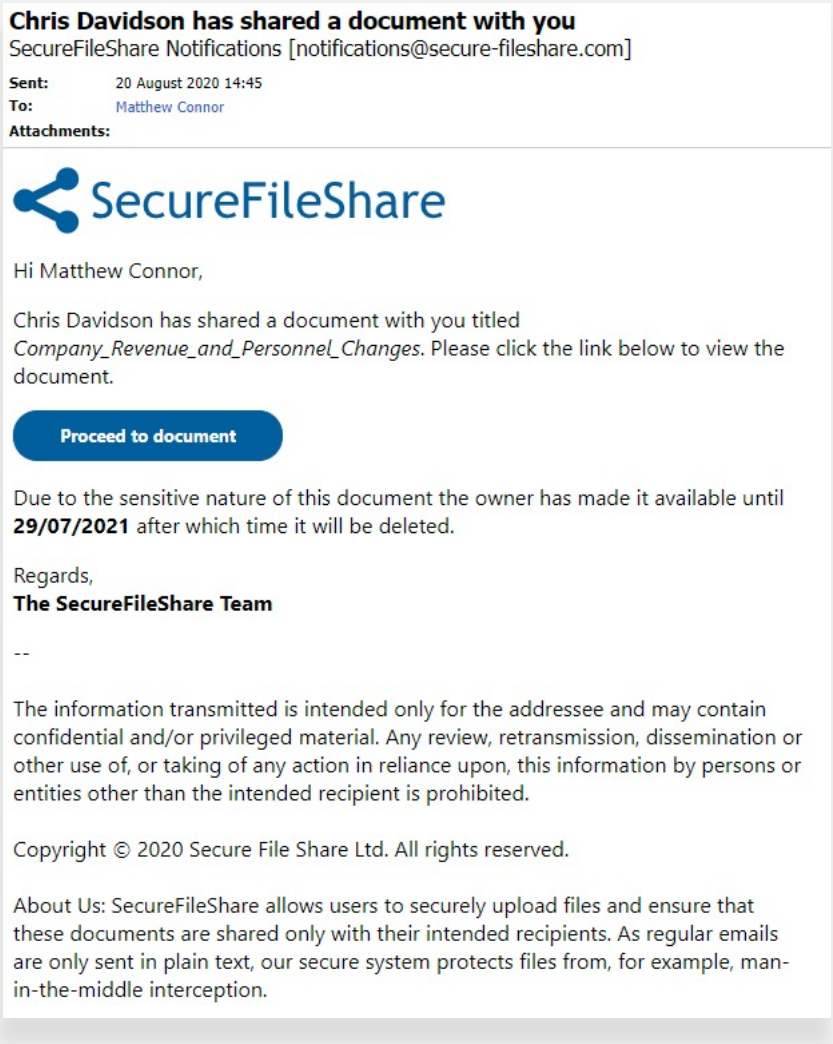
Could you urgently check have added their details correctly?

invoice_349862.pdf (349 KB)

Regards,

James Wright
Chief Financial Officer

Figure 2: Sample Document Share Email



Chris Davidson has shared a document with you
SecureFileShare Notifications [notifications@secure-fileshare.com]

Sent: 20 August 2020 14:45
To: Matthew Connor
Attachments:

SecureFileShare

Hi Matthew Connor,

Chris Davidson has shared a document with you titled *Company_Revenue_and_Personnel_Changes*. Please click the link below to view the document.

Proceed to document

Due to the sensitive nature of this document the owner has made it available until **29/07/2021** after which time it will be deleted.

Regards,
The SecureFileShare Team

--

The information transmitted is intended only for the addressee and may contain confidential and/or privileged material. Any review, retransmission, dissemination or other use of, or taking of any action in reliance upon, this information by persons or entities other than the intended recipient is prohibited.

Copyright © 2020 Secure File Share Ltd. All rights reserved.

About Us: SecureFileShare allows users to securely upload files and ensure that these documents are shared only with their intended recipients. As regular emails are only sent in plain text, our secure system protects files from, for example, man-in-the-middle interception.

Document Share

Document share emails are common and often use the familiarity with a brand to encourage the recipient to click. It can often be easier to mimic a notification from Microsoft or Google than it would be to spoof an internal email. To be effective, attackers only need to identify someone within the organization (ideally someone senior) and make the email appear to come from them. Often these types of attacks are used to capture corporate credentials as it is commonplace to log in to retrieve files from these types of document share applications.

For parity across organizations, we decided not to mimic a real document share service, but instead created a fictional document share company. Despite the company 'SecureFileShare' being fictional, we used a similar format and content from real document share notifications from well-known providers, adding some familiarity.

Internal HR Mimic

A very common and often effective email phishing attack. This email is designed to feel like a natural communication from the HR department about an everyday work issue. The issue is chosen to be one that would be expected from the HR department and, often, one that would be of great interest to the recipient. In this case we have chosen annual leave. However, salary adjustment, bonuses and organizational change are also common and effective.

An advanced attacker would likely design their email to feel very similar to a real internal email i.e., including a realistic signature, possibly appearing to come from a senior HR staff member. To be applicable to a wide audience we chose to use terminology that should feel natural but with a generic sender.

Figure 3: Sample Internal HR Mimic Email

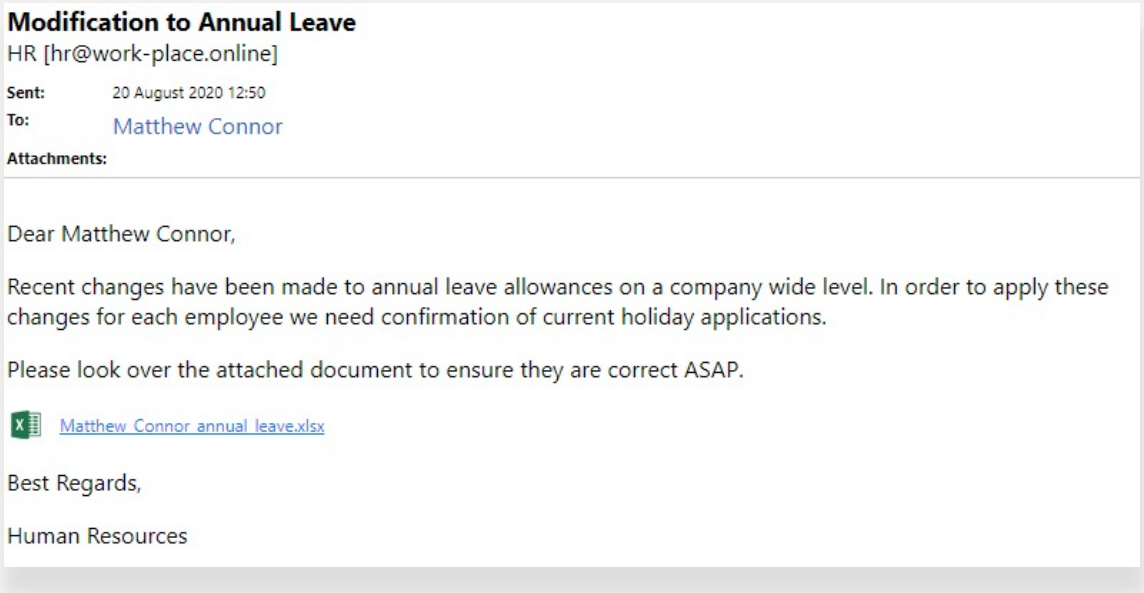
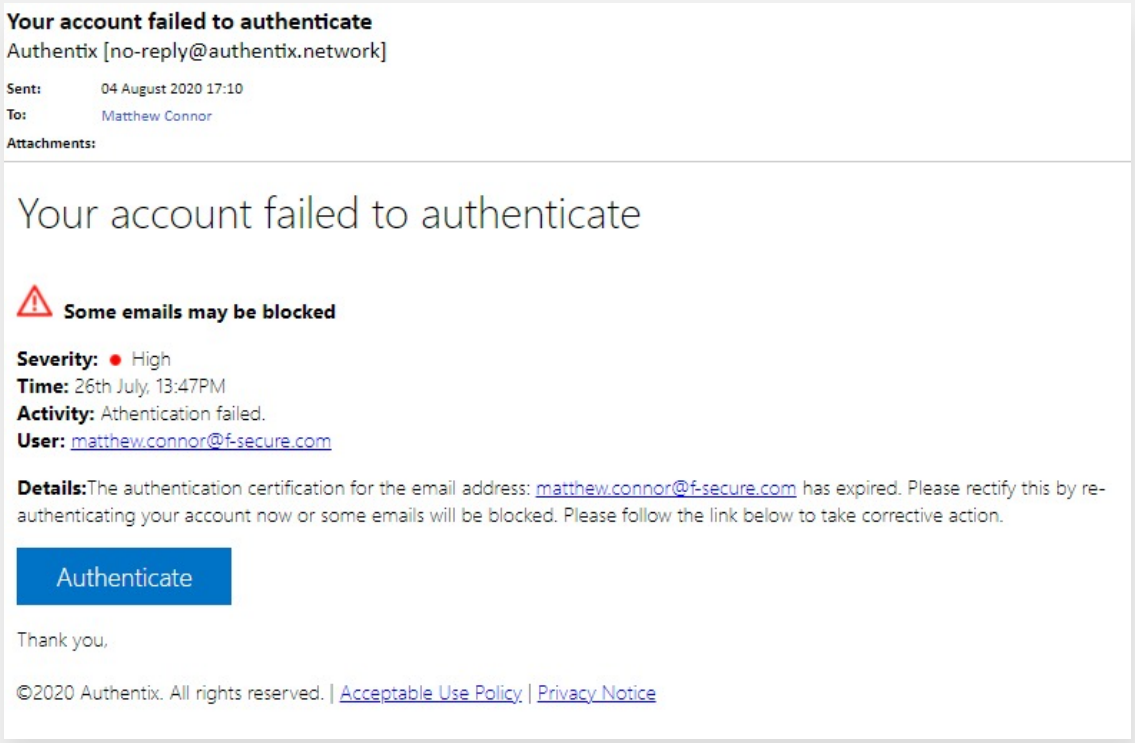


Figure 4: Sample Service Issue Notification Email



Your account failed to authenticate
Authentix [no-reply@authentix.network]

Sent: 04 August 2020 17:10
To: Matthew Connor
Attachments:

Your account failed to authenticate

Some emails may be blocked

Severity: ● High
Time: 26th July, 13:47PM
Activity: Athentication failed.
User: matthew.connor@f-secure.com

Details: The authentication certification for the email address: matthew.connor@f-secure.com has expired. Please rectify this by re-authenticating your account now or some emails will be blocked. Please follow the link below to take corrective action.

Authenticate

Thank you,

©2020 Authentix. All rights reserved. | Acceptable Use Policy | Privacy Notice

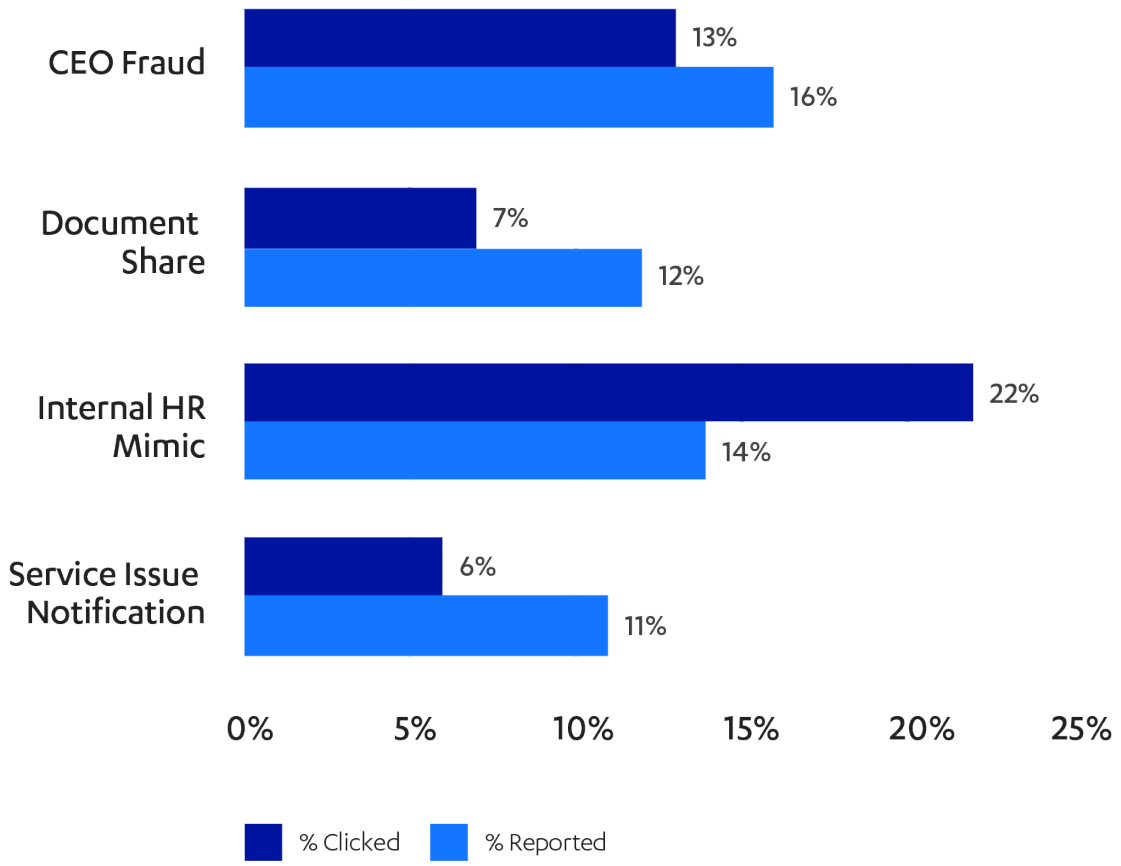
Service Issue Notification

As with document share emails, real service notifications are easy to mimic and utilize familiarity to encourage recipients to click. They often threaten small issues for the recipient rather than major ones. Because legitimate versions of these kinds of notifications are commonplace, some recipients may try to get rid of the problem quickly by doing what is asked without checking it first.

These emails regularly rely on trust in the purported sender to elicit clicks. However, as with the document share emails, we have created a service notification that looks and sounds familiar but is not from a known organization.

OVERALL RESULTS

Figure 5: Click/Report Rate per Email Type



The Internal HR Mimic email was the most effective in eliciting a click. There may be many reasons for the difference between the click rate of the different emails sent. However, F-Secure assess that the inclusion of personal impact in the HR email was a substantial factor for its high click rate. Internal HR Mimic used loss aversion and authority as well as benefiting from being sent in early 2021 when the COVID-19 pandemic meant organizations were more likely to make large scale changes.

F-Secure assess that the Document Share and Service Issue Notification emails not being branded to a well-known and used service likely affected their click rate. Security teams should be aware that a real attacker might mimic a well-known service and have more success.

CEO Fraud was the most reported email at 16% of recipients reporting it as suspicious. This may be because the idea of receiving an email directly from a very senior member of staff is something to take note of. Given its novelty users might have explored the email further, identifying the external tag or other flags of illegitimacy. These kinds of attacks have also featured heavily in the media, meaning recipients may be more aware of their malicious nature.

Figure 6: Click Rate per Email Type and Organization

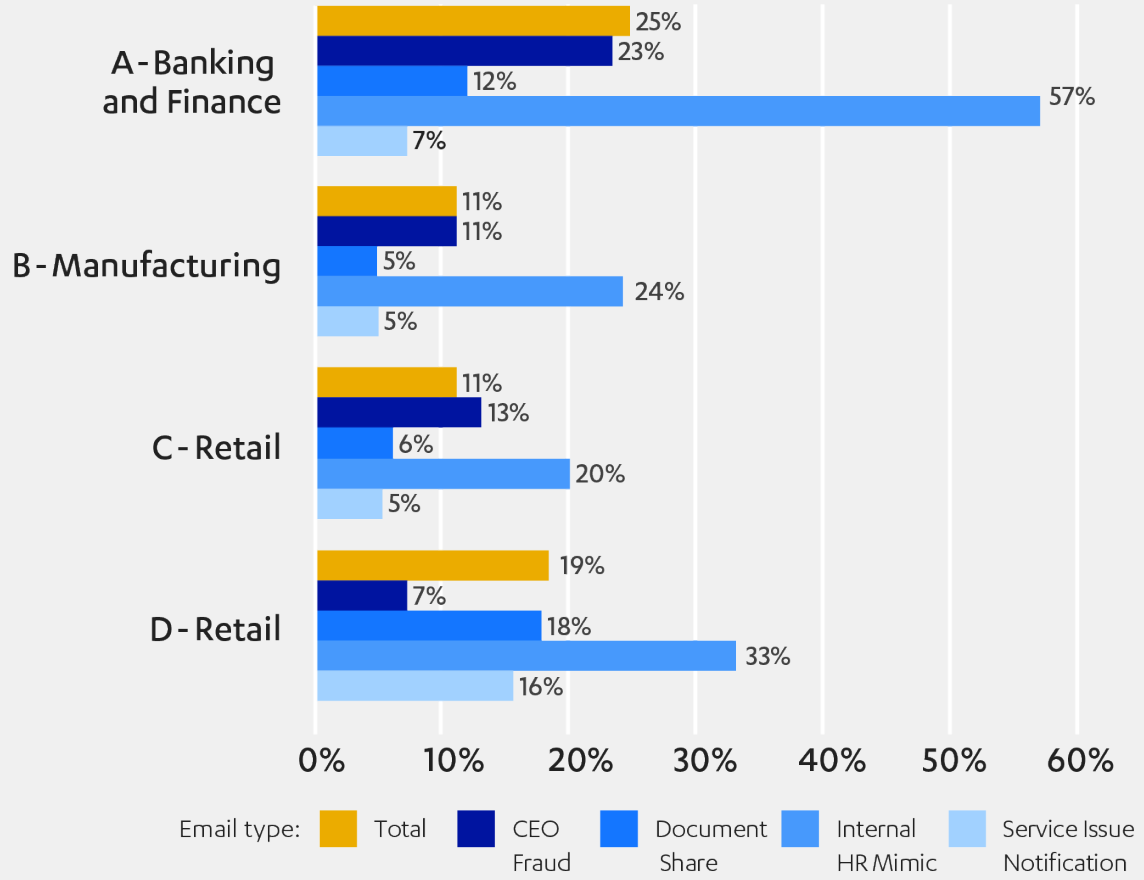
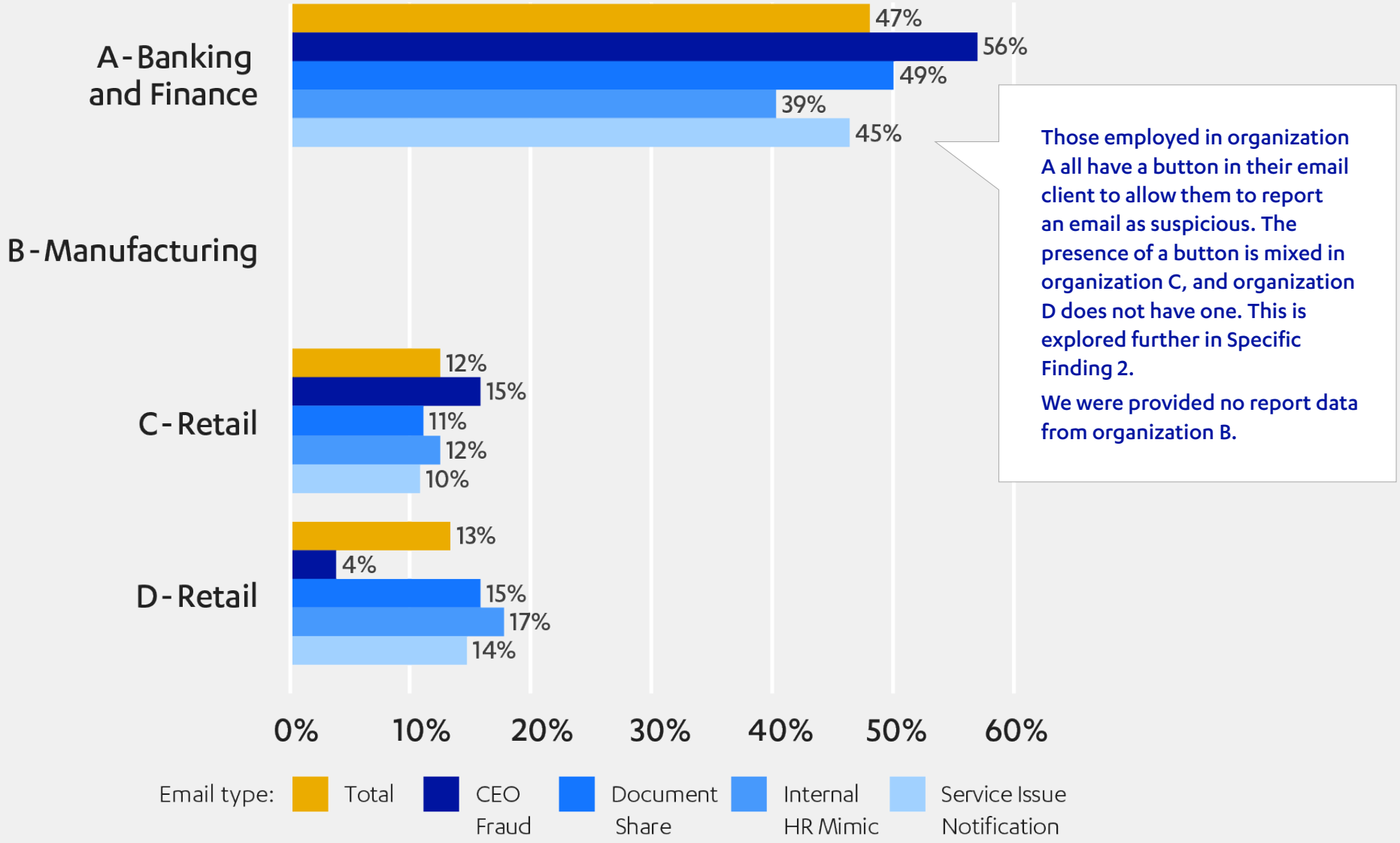


Figure 7: Report Rate per Email Type and Organization

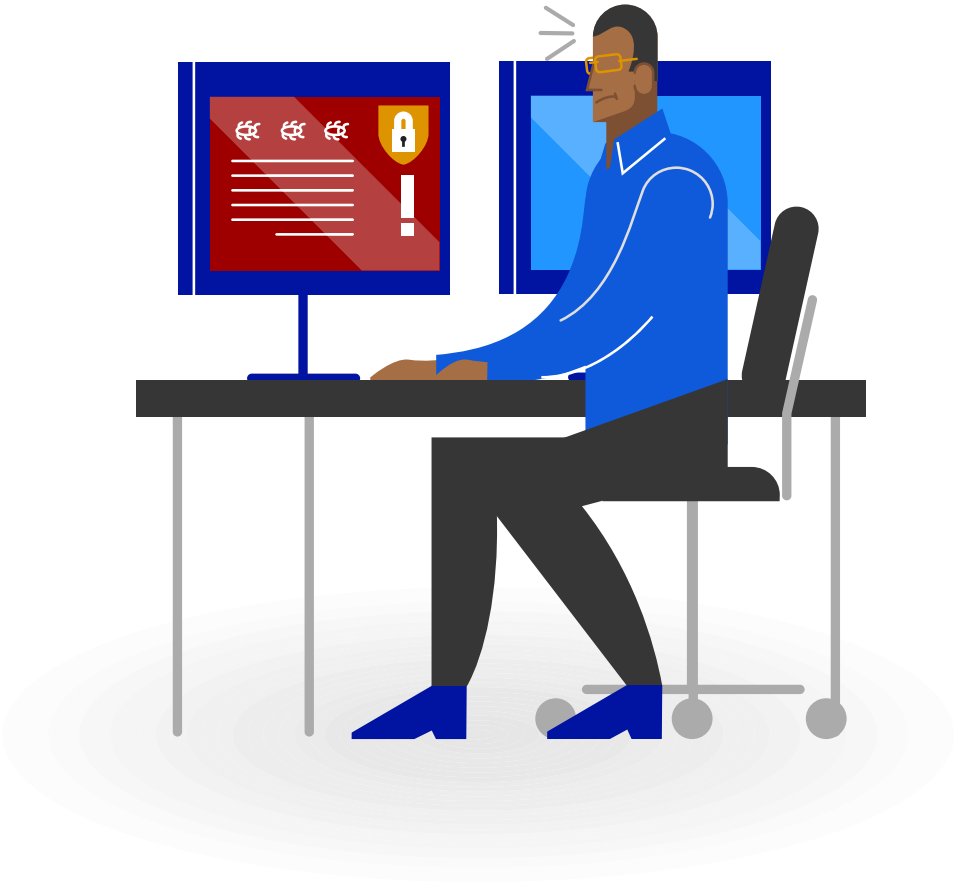


Those employed in organization A all have a button in their email client to allow them to report an email as suspicious. The presence of a button is mixed in organization C, and organization D does not have one. This is explored further in Specific Finding 2.

We were provided no report data from organization B.

SPECIFIC FINDING 1

Staff employed in IT related roles are no less susceptible to phishing than the rest of the organization.



Those employed in roles within IT and DevOps departments were no less susceptible to phishing than those in other areas of the business. Both organizations A and C provided department data that included IT and DevOps. In both organizations these departments were similarly susceptible to the rest of the business. In organization A 26% of DevOps and 24% of IT showed susceptibility compared to 25% of the organization overall. In organization C, 30% of DevOps and 21% of IT showed susceptibility compared to 11% of the organization overall. All organization A employees are UK based, but organization C has employees in several different countries, including those employed in IT and DevOps. In most locations these employees remained at least as susceptible as the rest of the organization and in many, far more susceptible (tables with data follow). In addition, IT and DevOps were no better at reporting the emails as suspicious as the rest of the business.

When asked, more staff in both IT and DevOps in organizations A and C reported noticing a phishing attack in their inbox in the past than the rest of their organization:

In organization A, overall, 17% of clickers reported to have noticed a phishing attack in their inbox in the past. In IT the number was 27% and in DevOps that number is 29%.

In organization C, overall, 44% of clickers reported to have noticed a phishing attack in their inbox in the past. In IT the number was 49% and in DevOps that number was 60%.

This suggests that staff in IT and DevOps believe themselves able to identify a phishing email, more so than the other areas of their businesses. This judgement is arrived at through self-reporting after having clicked on a phishing simulation, so their recollection may be affected. This number should also be balanced against the possibility that IT and DevOps receive more phishing attacks than other parts of the business so have had more opportunities to identify them.

There is an assumption that those who are more technically focused will be better placed to identify and respond appropriately to phishing attacks. However, the results of this study suggest otherwise. F-Secure believe there are two key implications of this outcome:

Given the additional access or permissions people in technical roles are likely to have, it is critically important to apply the best protective measures around them. **Their advanced technical knowledge will not make them less susceptible to phishing.**

If we believe that staff in IT and DevOps are some of the most knowledgeable about phishing attacks, our results suggest that **knowledge is insufficient to prevent susceptibility to phishing attacks.**

"We are human first and we are our role second."

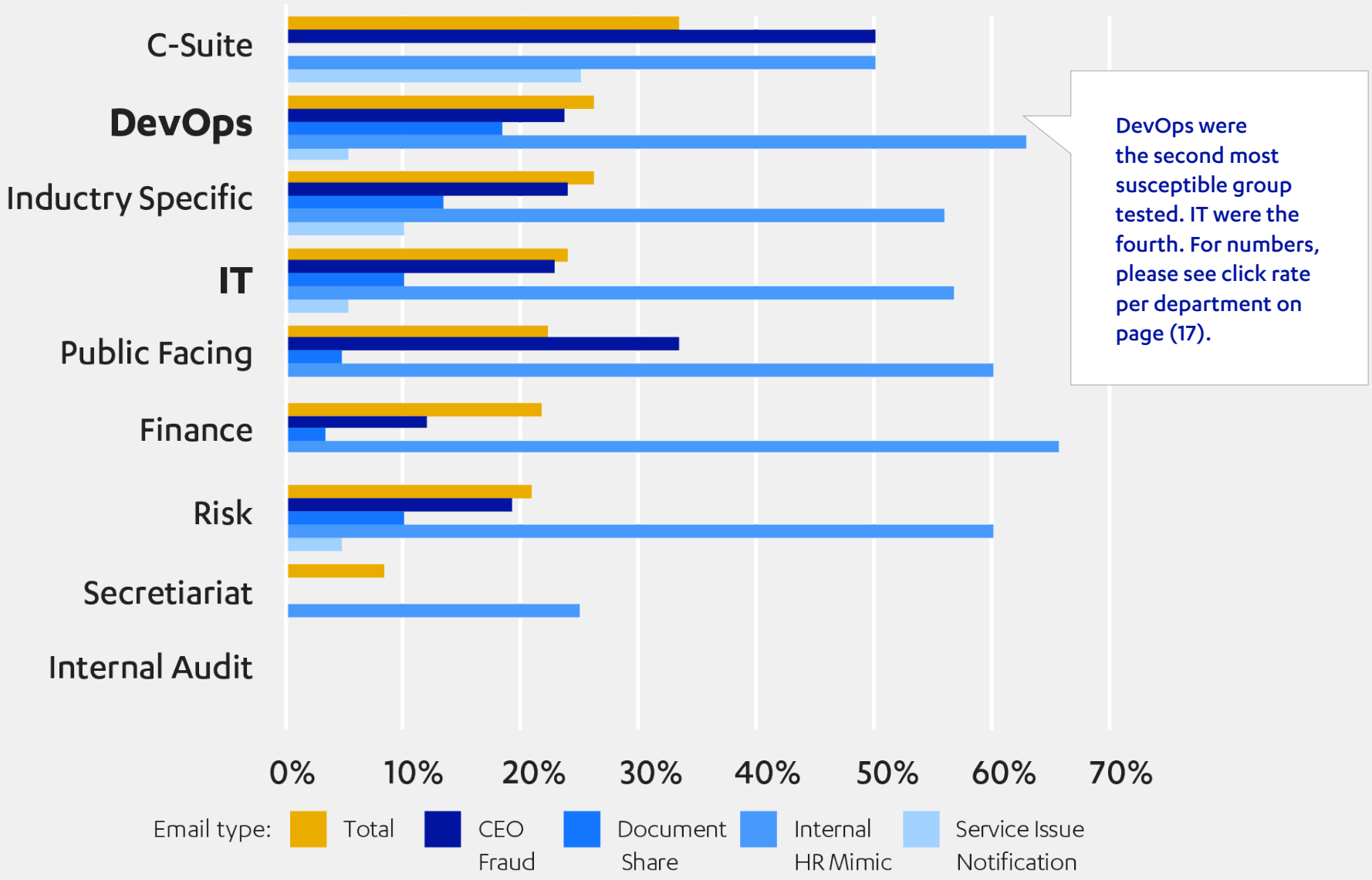
Riaan Naude
Director, F-Secure

Hopefully the guidance from the first implication should be clear – protect your technical staff from phishing attacks but expect them to fall victim just like anyone else. The second implication, however, needs further examination. If knowing about the impact of phishing attacks, how to spot them and what to do when you do spot them is insufficient to prevent susceptibility to them, how should the industry respond?

We believe that simply educating staff is insufficient to reduce an organization's risk from email phishing. Each organization should consider carefully what options are available and are suitable to reduce the risk posed. Providing occasional phishing awareness education will not substantially reduce the risks. F-Secure is not suggesting that phishing awareness education is valueless, only it should form part of a complete and cohesive approach to limit the risks an organization faces.

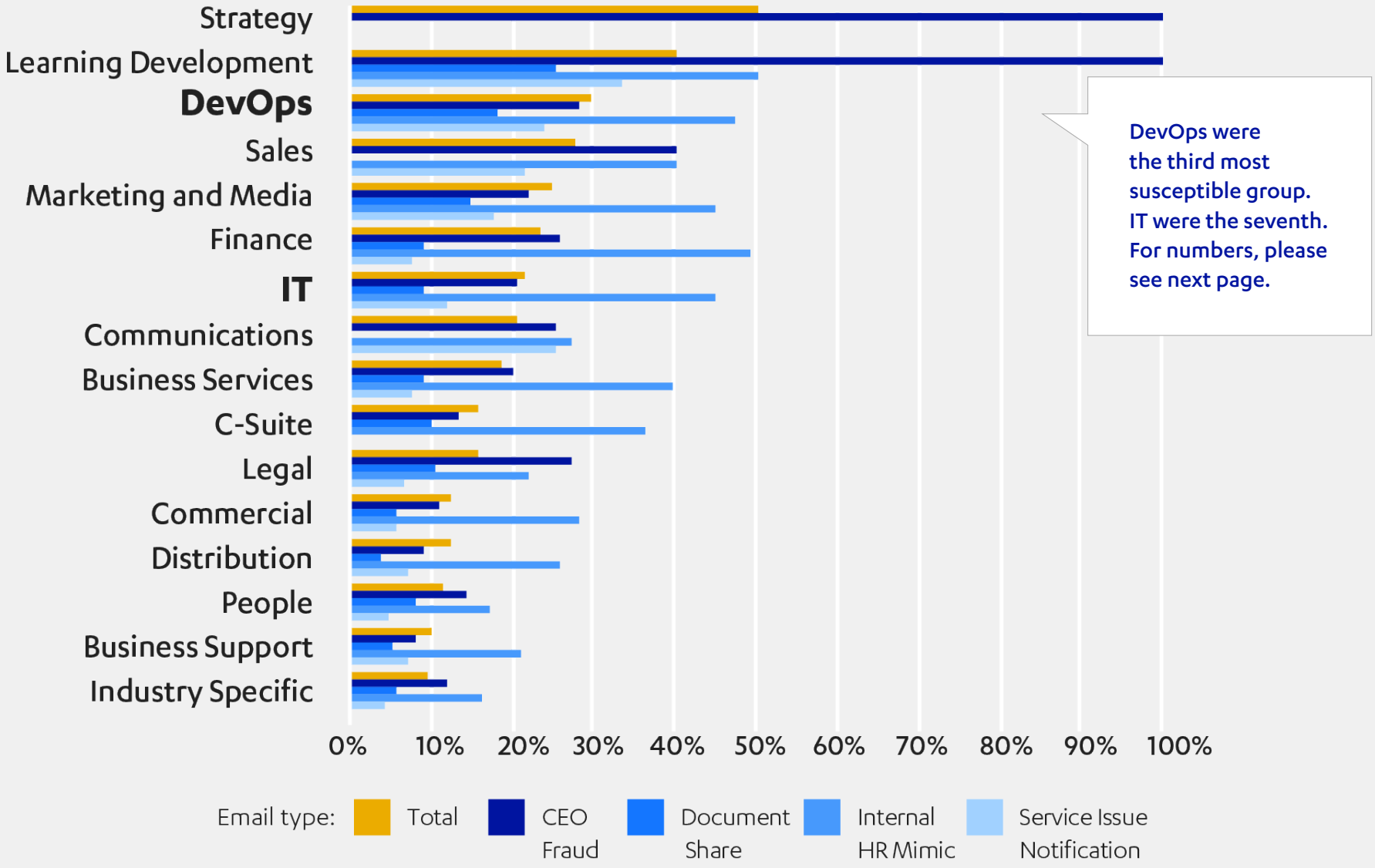
SPECIFIC FINDING 1 - EVIDENCE

Figure 8: Click Rate for Organization A per Department and Email Type



DevOps were the second most susceptible group tested. IT were the fourth. For numbers, please see click rate per department on page (17).

Figure 9: Click Rate for Organization C per Department and Email Type



Click Rates by Department

Figure 10: Click Rate for Organization A per Department

Department	Clicks %	Clicks #
C-Suite	33%	4 of 12
DevOps	26%	63 of 240
Industry Specific	26%	392 of 1496
IT	24%	145 of 604
Public Facing	22%	23 of 103
Finance	22%	27 of 124
Risk	21%	29 of 139
Secretariat	8%	1 of 12
Internal Audit	0%	0 of 15

Figure 11: Click Rate for Organization C per Department

Department	Clicks %	Clicks #
Strategy	50%	3 of 6
Learning and Development	40%	4 of 10
DevOps	30%	293 of 991
Sales	28%	11 of 40
Marketing and Media	25%	240 of 971
Finance	23%	385 of 1668
IT	21%	853 of 3972
Communications	20%	12 of 59
Business Services	19%	490 of 2619
C-Suite	16%	7 of 45
Legal	15%	16 of 104
Commercial	12%	16 of 130
Distribution	12%	15 of 123
Business Support	12%	77 of 655
People	11%	93 of 833
Industry Specific	9 %	5778 of 61558

Organization A is entirely UK based. However, organization C has staff spread across the world. These are the IT and DevOps click rates geographically. While there is some variation between the larger groups tested, most showed broadly similar levels of susceptibility. This suggests the issue of susceptibility is not bound to a certain national culture but persists across the entire department.

Figure 12: Click Rate for Organization C's IT Staff per Country

Country	Clicks %	Clicks #
South Africa	100%	1 of 1
Thailand	55%	6 of 11
Italy	50%	1 of 2
Malaysia	50%	1 of 2
Norway	50%	1 of 2
Japan	40%	2 of 5
USA	39%	12 of 31
Brazil	33%	6 of 18
Colombia	33%	1 of 3
France	33%	1 of 3
Slovakia	33%	2 of 6
Czechia	33%	30 of 91
Canada	29%	2 of 7
Poland	29%	2 of 7
China	25%	2 of 8
India	23%	543 of 2374
UK	18%	235 of 1342
Hungary	15%	2 of 13
Ireland	9%	3 of 33
Chile	0%	0 of 1
Turkey	0%	0 of 1
Sri Lanka	0%	0 of 1
Spain	0%	0 of 1
Hong Kong	0%	0 of 4
Korea, Republic of	0%	0 of 5
IT Total	21%	853 of 3972

Figure 13: Click Rate for Organization C's DevOps Staff per Country

Country	Clicks %	Clicks #
Germany	100%	1 of 1
Italy	100%	1 of 1
Russia	100%	1 of 1
USA	42%	14 of 33
Poland	40%	2 of 5
Hungary	33%	1 of 3
India	30%	163 of 549
UK	28%	110 of 392
Brazil	0%	0 of 2
Canada	0%	0 of 2
France	0%	0 of 1
Ireland	0%	0 of 1
DevOps Total	30%	293 of 991

Figure 14: Report Rate for Organization A per Department and Email Type

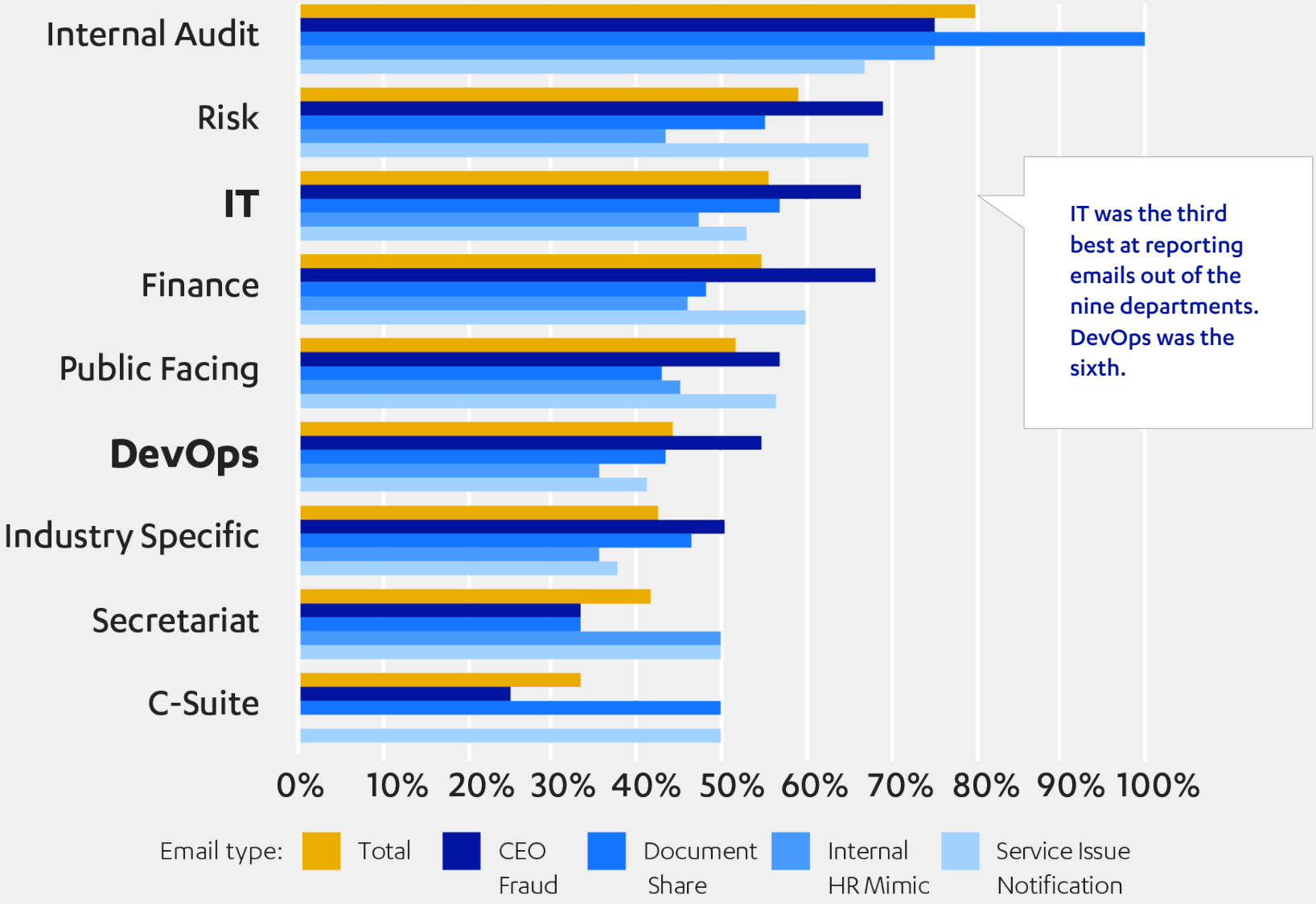
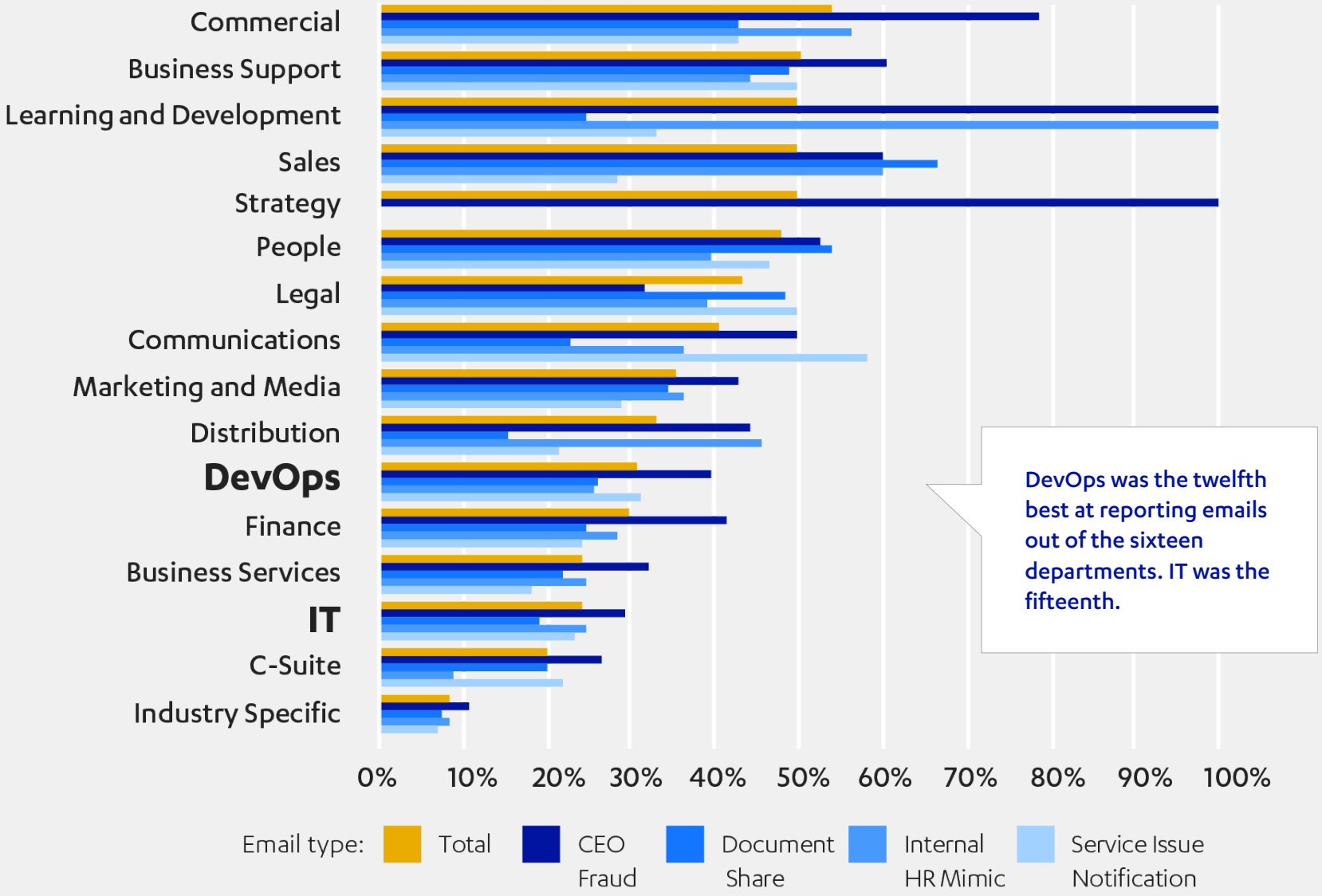


Figure 15: Report Rate for Organization C per Department and Email Type



SPECIFIC FINDING 2

The number of suspicious emails that are reported is directly influenced by the process of reporting an email.

Those with a button to report emails as suspicious in their email client reported our study emails far more than those without a button.

Organization A has a reporting button. Organization B did not provide us with reporting information. Staff in organization D do not have access to a reporting button. Only two groups within organization C have a reporting button. 47% of staff in organization A reported the emails as suspicious while organizations C and D staff only reported 12 and 13%, respectively. While we should expect different working patterns in different organizations to impact report rate, by exploring those within organization C we can see the value of a reporting button.

In organization C some employees had access to a reporting button while most did not. 44% of those with access to the button reported the test email as suspicious. Only 11% of those without the button reported the email. This should be a clear indication that a single simple method for reporting emails as suspicious is essential if you want your staff to provide a line of defense against phishing.

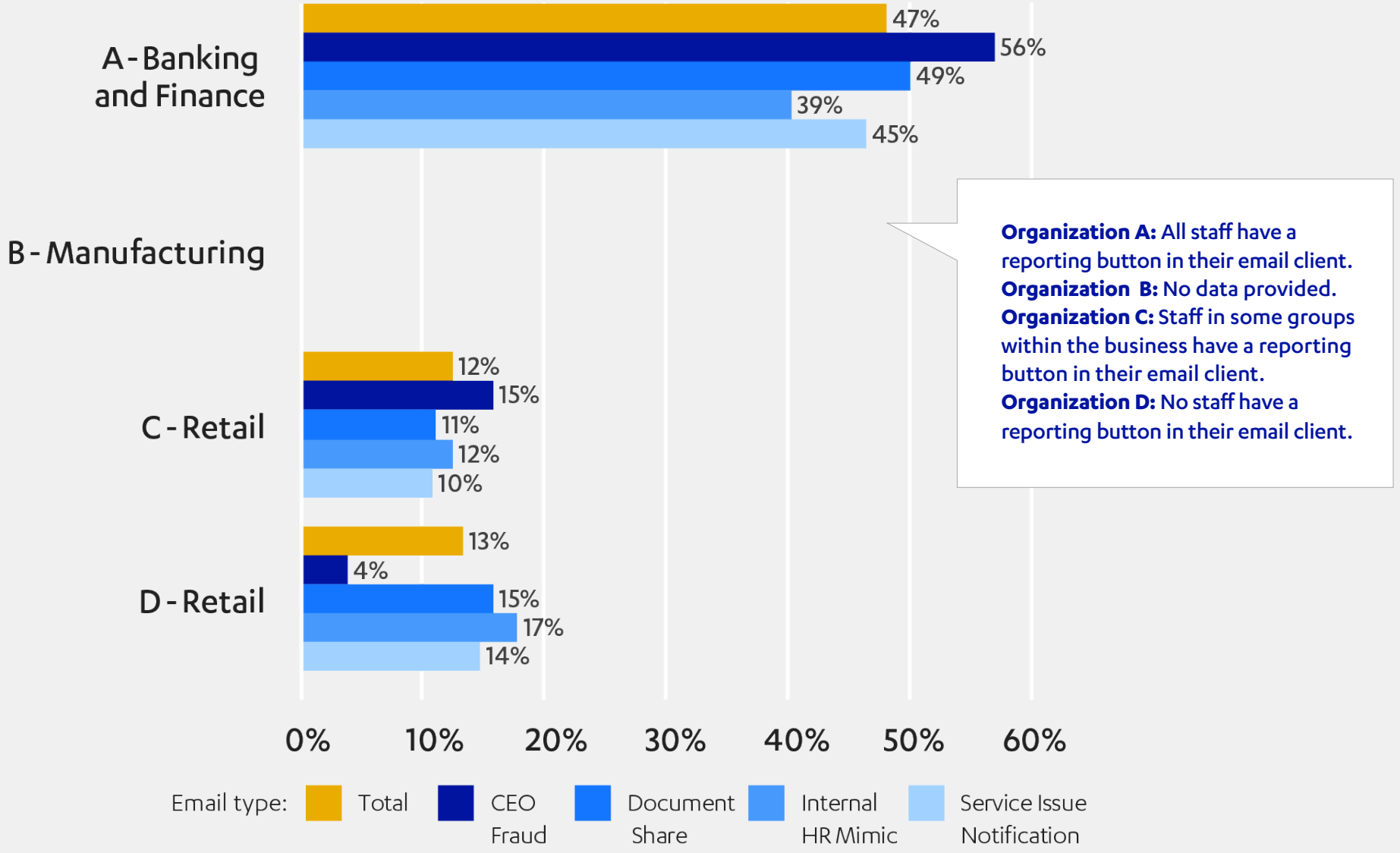
To those in a security center struggling with an already high case load, the prospect of quadrupling the number of reported emails may be unpalpable. The solution, however, is in automation.

"It's all about making the reporting process as quick and easy as possible. The quicker and easier it is for an end user to report a suspicious email, the more likely they are to actually do it."

Chris Maley
Head of Delivery, F-Secure Phishd

SPECIFIC FINDING 2 - EVIDENCE

Figure 16: Report Rate per Organization and Email Type



SPECIFIC FINDING 3

Speed is critical for all parties in an attack.

In the first minute after the emails arrived in inboxes, over three times the number of people who reported it as suspicious had clicked. This number leveled out at around 5 minutes and stayed consistent across the time periods after that.

Figure 17: # of Clicks/Reports by Time from Email Delivery

	# Clicked	# Reported
1 minute	860	258
5 minutes	2,008	1,819
30 minutes	3,736	3,864
1 hour	4,537	4,722
24 hours	7,081	6,780

A quarter of all those fell victim to our simulation emails clicked within 5 minutes of receiving it.

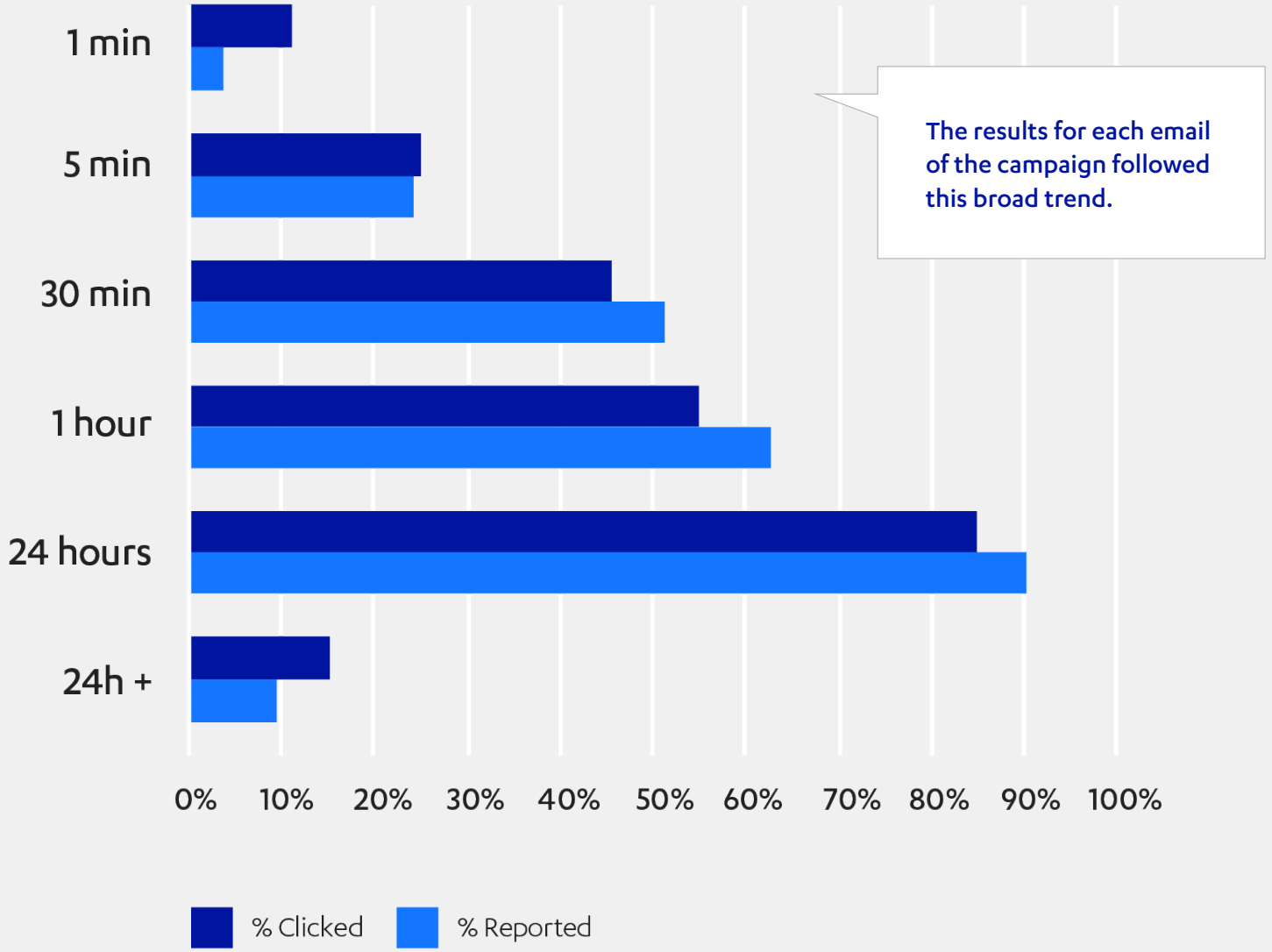
For every phishing email a SOC receives it should expect that someone has fallen victim to it within the business. They should have the ability to identify any other instance of that email and to take mitigative actions. This action must be taken quickly as within 30 minutes of receiving an email 50% of those people who are going to click will have clicked. 30 minutes is a long time for an attacker to undertake damaging activities within your network.

"If you don't respond to things quickly then you have to expect that you are going to get malware detonation and you will need to deal with it at the next stage, at which point you'll have to step up your game."

"The speed at which an attacker can get a shell back is perhaps just 4 or 5 seconds. It's that quick".

Matthew Pendlebury
Former Managing Consultant and Information Security Manager F-Secure Consulting

Figure 18: Click/Report Rate by Time from Email Delivery



APPENDIX - STUDY CHOICES

There were several concessions made in the planning and preparation of this study which will have had an impact on the results.

Email Content:

Well-designed phishing emails will be targeted towards the recipient or at least be appropriate for that audience. As we were targeting entire organizations with staff in significantly different roles, we had to adjust the emails to be broadly appropriate for all recipients. Because of this adjustment the emails were less effective than emails targeted towards individual roles could have been.

Email Delivery Time:

Similar to email language, we could not deliver emails exactly within the working hours of every country. As the majority of the recipients across all organizations were based in the UK, we decided to send all emails between 10:00 and 15:00 GMT.

Email Design:

The CEO Fraud and Internal HR Mimic email both purported to come from a colleague inside the recipient's business. We decided not to mimic an internal sender for these as it might create inconsistencies between the different organizations.

Similarly, Document Share and Service Issue Notification emails often rely on the familiarity of the service in selling the conceit. As each target organization may use different services, we decided to use fictional companies for each. F-Secure believes that if these emails had mimicked a real service that is used by the recipients, the click rate would have been higher.

Email Language:

As English was the primary professional language of all the companies targeted, we made the decision not to translate emails into local languages.

Allow-Listing:

All emails sent were allow-listed, meaning none were prevented from reaching the recipients by technical protections.

ABOUT F-SECURE

Nobody has better visibility into real-life cyber attacks than F-Secure. We're closing the gap between detection and response, utilizing hundreds of our industry's best technical consultants, millions of devices running our award-winning software, and ceaseless innovations in artificial intelligence. Top banks and enterprises trust our commitment to beating the world's most potent threats. Together with our network of the top channel partners and over 200 service providers, we're on a mission to make sure everyone has the enterprise-grade cyber security we all need.

Founded in 1988, F-Secure is listed on the NASDAQ OMX Helsinki Ltd.

f-secure.com | **twitter.com/fsecure** | **linkedin.com/f-secure**

F-Secure