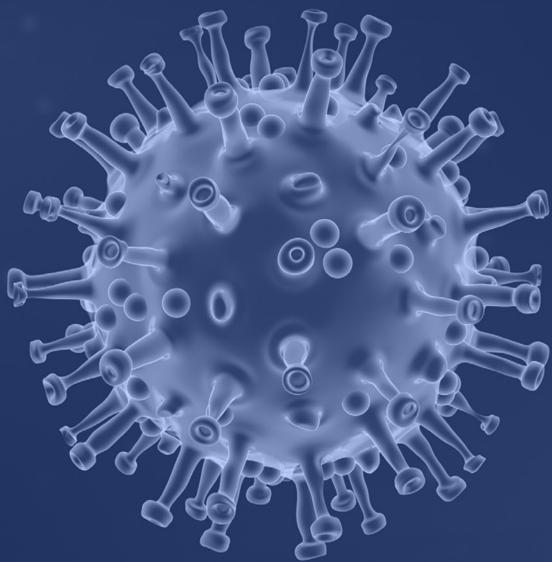
The 2021 Phishing Intelligence Report

report by PHISHED

Table of contents

1. Key Learnings

Without thorough prior education, **1 out of 2** employees is susceptible to phishing.



COVID-19-related communication is the most notorious subject in a successful phishing campaign.

23%

of employees who are phished then **enter data** into spoofed landing pages.

7% of all employees open possibly dangerous **email attachments**.

2. Introduction: General Observations For 2021

The 2020 health crisis, a.k.a. the **coronavirus pandemic**, marked the starting point of a significant rise in the popularity – or notoriety – of phishing attacks. As a phenomenon, the pandemic continued to influence every part of our daily lives throughout 2021. Meanwhile, hackers and other malicious actors have **efficiently adapted** their 'best practices' to encompass new and previously uncommon **ways of life and work**.

The alterations were, among others, caused by:

- Increased **anxiety, fears and emotions** because of COVID-19
- **Inexperience** with working from home, both from the perspective of employees and employers
    - Includes the necessity to quickly implement and train users in new software tools and protocols
- Stark increase in
    - Online shopping
    - Online servicing (government, banking, providers,...)
    - Fake news (COVID measures, vaccination information,...)

As the public faced sudden changes in both their personal and professional environments, it became a lot easier for malicious actors to enter the field of cybercrime:

- **Phishing kits** are available at ever-declining prices. They are easy to use out-of-the-box and are lowering the difficulty threshold for anyone willing to take the risk.
- **Databases** are becoming more available, in part because of insufficient protection by data gatherers, such as social media platforms. 2021 alone saw media report over **1 billion users' data scraped** on two of the largest platforms in the world.
- **Channel diversification**: it is becoming easier to diversify phishing attacks. The cost per SMS (smishing) declines every year, while the software to exploit it is becoming cheaper and easier to use as well. Voice phishing (vishing) is becoming trickier to recognise because of a more **localised approach** by threat actors.

Did you know?

'People don't think, they click', especially when:

- The phishing message is **short** and to the point
- The message contains a **request for help**
- The sender appears to be **known** to the recipient (chances of a click rise by **30%**!)
- The phishing message contains a reference to a **hot topic**

The coronavirus pandemic has decisively and permanently opened the door to a continuous rise in phishing threats. As they form the basis for the vast majority of all cyber breaches, it is important for people to realise what the dangers are, how to recognise them and how to deal with them.

That is why Phished presents its **'Phishing Intelligence Report'** of 2021.

Happy reading,
Arnout Van de Meulebroucke
CEO Phished

3. A Word On Phished And The Database

3.1. Who is Phished?

Phished focuses on the **human side of cybersecurity**. The AI-driven training software combines personalised, realistic phishing simulations with the educational program of the Phished Academy. This way, your employees are qualified to correctly and safely deal with online threats. Because employees are better prepared and more secure, the data, reputation and assets of organisations are more secure as well.

3.2. The Phished Software And Database

90% of all data breaches start with a human error. Mistakes that can lead to viruses, ransomware, theft of money and data, and the loss of reputation. Phished trains your co-workers to handle cyber threats efficiently, effectively and within a safe and controlled environment.

The data in this report was accumulated by sending millions of phishing simulations to hundreds of thousands of **recipients worldwide**.

Building the human firewall at PHISHED

4. Phishing Globally

Everyone, in every corner of the world, in every industry or sector, in any job is vulnerable to phishing. That has once again been proven when looking at the global Phished statistics for 2021. An overview of the key statistics for Phished recipients on a global scale.

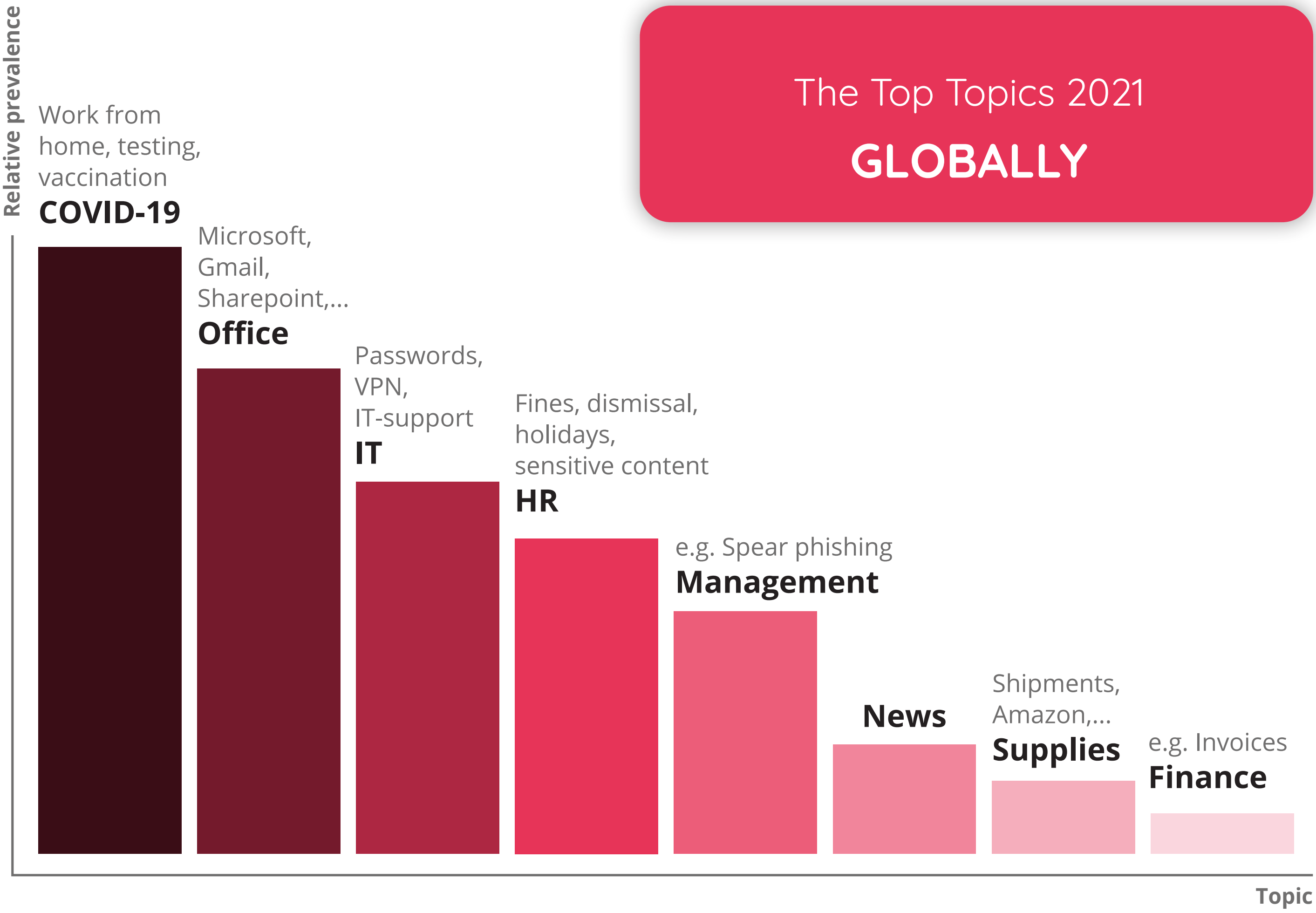
4.1. Most Popular Topics

Following last year's trend, COVID-19 once again tops the global ranking. Unsurprisingly so, given the broad information and vaccination campaign that touched most citizens in most countries. The many fake news and misinformation campaigns fuelled malicious actors to tap into the general anxiety about the risks of vaccines and side-effects.

Following closely behind are office-related emails, comprising everything from issues with Microsoft Office tools, login prompts from Gmail, and broader IT-related phishing messages containing password queries, IT support and VPN.

HR-related messages form a notable category as it managed to lure many people into the phishing trap. Many of these messages reference employees' holidays, while Not Safe For Work (NSFW) messages fall into this category as well: they involve fines, dismissals or mention pornographic aspects.

A special mention goes to financial messages (e.g. pertaining to unpaid invoices): they form an important part of all successful phishing messages, but less so than generally assumed.



4.2. How Vulnerable Is The Average Employee?

Phished sends out millions of phishing simulations on an annual basis. Organisations can choose the intervals, but on average a recipient will receive 1 simulation per 10 days.

Globally, **22%** of all simulations are successful. Taking only opened phishing messages into account, this surges up to **53%**.

If a simulation contains the possibility of data entry (e.g. on a spoofed login page), **23%** of all victims enter their data.

If a message contains an attachment, **7%** of all recipients will download and open it.

Phishing messages are not often replied to: only **0.55%** of all recipients answered a simulation.

7% successfully reported the simulation.

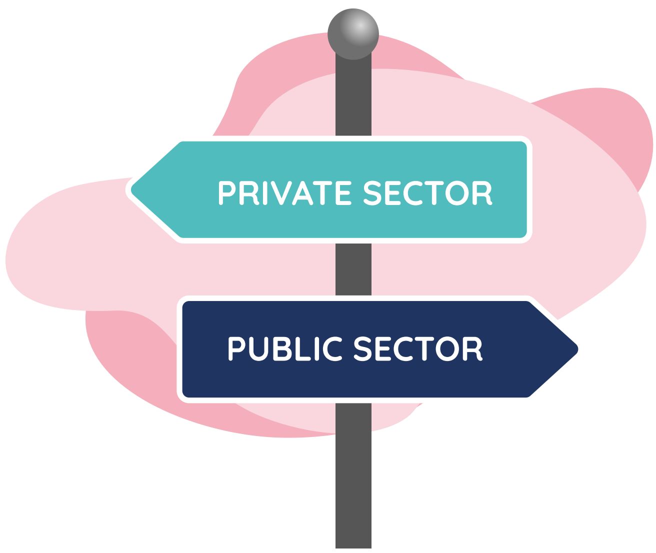
Phished (of sent)	Phished (of opened)	DataEntry (of opens)	DataEntry (after being Phished)	Replied	Attachment	**Reported**
21,63%	52,90%	5,11%	23,33%	0,55%	7,15%	**6,85%**

4.3. Public vs. Private Sectors

There is a distinct difference in how the public sector (has to) handle cybersecurity compared to the private sector.

Since public institutions are often funded with public money, they are, for example, bound to strict and rigorous selection criteria when selecting their cybersecurity awareness programs.

While it's difficult to determine whether that's a differentiating factor when comparing both fields, the fact remains that employees in the public sector fall into the phishing trap **3% more often** than those in private sector organisations.



5. Phishing in the UK

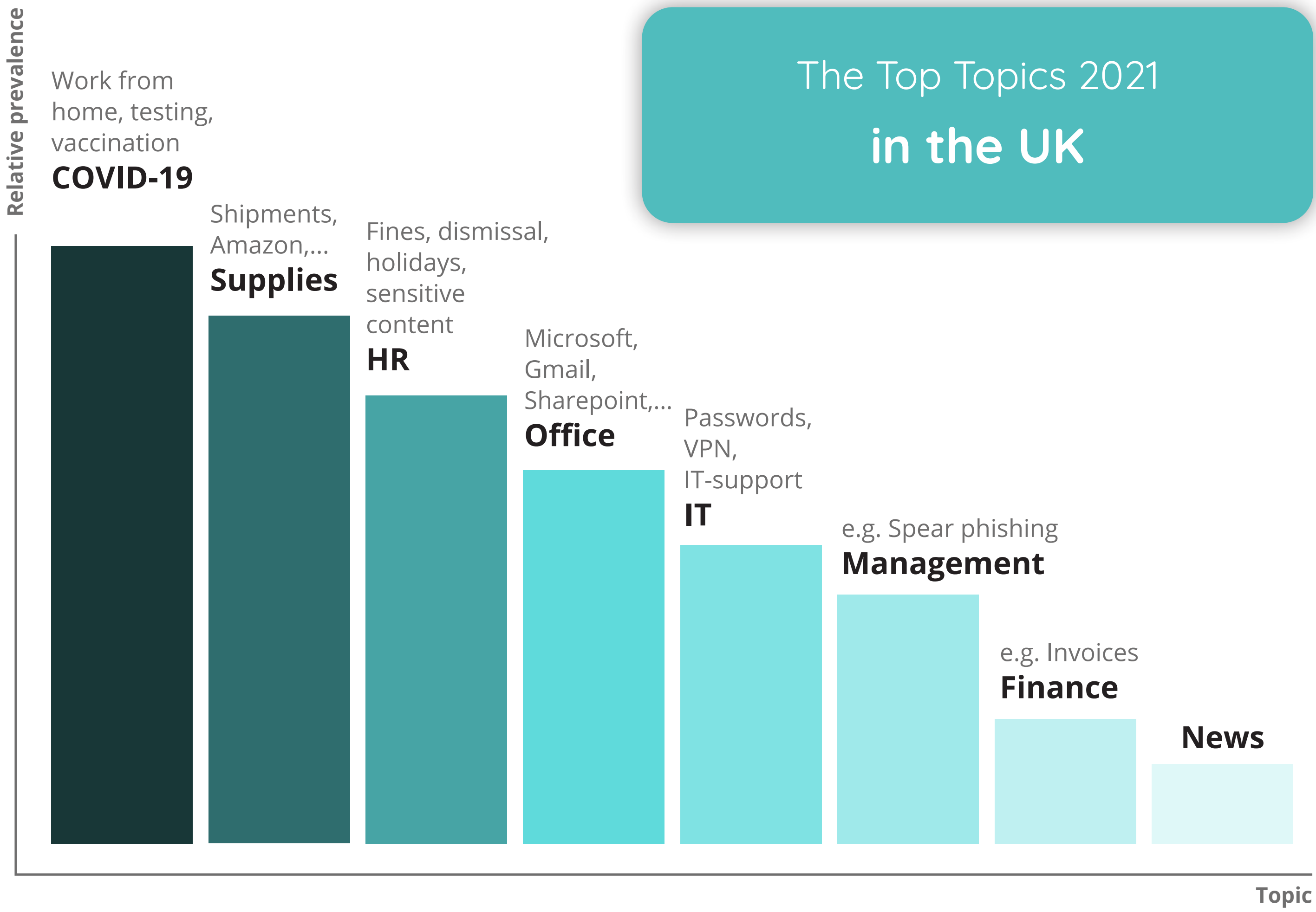
5.1. Most Popular Topics

Although the most popular topic in the United Kingdom for 2021 is, predictably, the same as for the global list – COVID-19 continues to keep the entire world in its grasp – places two through eight differ substantially.

The most notable difference being the second place for supply-related topics. Package delivery plays an important role here, given that online retail companies have a large footprint in the UK. Since the Phished algorithm automatically learns its recipients fields of interest, this means that UK employees are falling into the trap more often when a message is apparently coming from package delivery companies, because they show an increased interest in this type of message compared to the global average.

HR-related messages take up third place; many of these simulations reference employees' holidays, while sensitive content falls into this category as well: they involve fines, dismissals or mention pornographic aspects.

Simulations pertaining to IT topics are noticeably less successful when compared to the global average, which means that UK employees are slightly less likely to fall for phishing messages claiming problems with corporate tools or password violations.



5.2. How Vulnerable Are UK Employees?

Compared to the overall results, UK employees are generally speaking on par with their global counterparts. The differences are minimal and only become visible when looking beyond the rounded percentages.

In the UK, **22%** of all simulations are successful. Taking only opened phishing messages into account, this surges up to **53%**.

If a simulation contains the possibility of data entry (e.g. on a spoofed login page), just over **23%** of all victims enter their data.

If a message contains an attachment, **7%** of all recipients will download and open it.

Phishing messages are not often replied to: only **0.6%** of all recipients answered a simulation.

Over 7% successfully reported the simulation, slightly more than the global average.

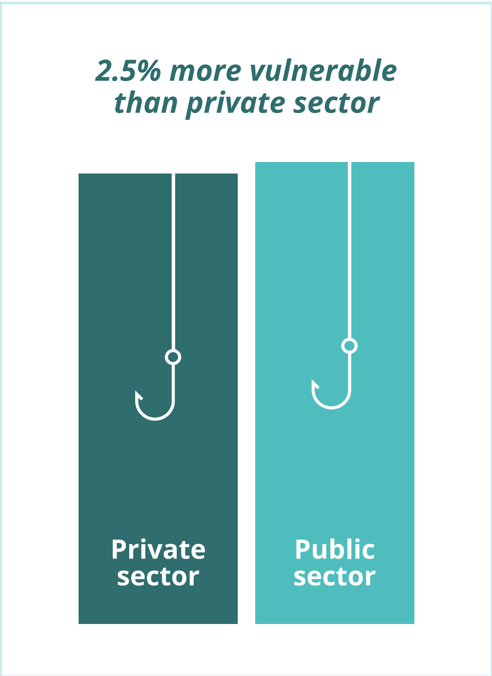
Phished (of sent)	Phished (of opened)	DataEntry (of opens)	DataEntry (after being Phished)	Replied	Attachment	Reported
21,70%	52,64%	5,00%	23,45%	0,60%	6,72%	7,74%

5.3. Public vs. Private Sectors

As in the global results, the UK public sector is slightly more vulnerable to phishing than private sector organisations:

Employees in the public sector fall into the phishing trap **2.5% more often** than those in the private sector.

This is just under the global average of **3%**.



6. Performance With Phished

When new clients start using the Phished platform to train their employees, the first simulation to reach recipients will most often be a general test, often referred to as the 'baseline measurement test'.

Over the past year, Phished concluded that, on average, **45%** of all recipients were phished during the initial baseline test. If the test included a data entry part, **27%** entered personal information (login data, unique ID's,...).

In one case, Phished managed a success ratio of **100%**: this was a baseline measurement where the client provided inside information that was, at the time, a recurring topic of conversation.

This result highlights the danger of insider threats. A hacked employee mailbox could potentially lead to a comparable outcome.

7. Trends for 2022

While new trends surface regularly, most successful phishing attacks are variants on older campaigns or repurposed campaigns that have proven successful in the past. That is why it is of paramount importance that companies start by training their people on the basics:

The fundamental issues with phishing and how to recognise them.

Anti-phishing training is about learning general principles that help protect people against more specific threats. 2022 will see the continuation of the most popular trend today: **COVID-19-related** communication.

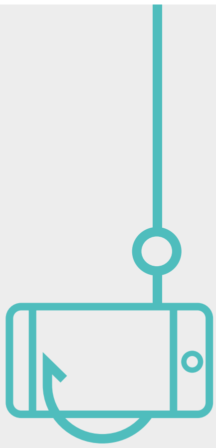
Nevertheless, there are some new and re-invented phishing strategies on the horizon as well.

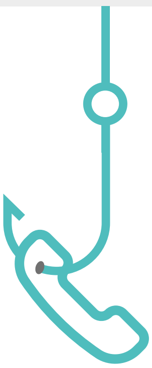
Deepfakes

Deepfakes are becoming relatively easy to create in just a matter of seconds, on any smart device. They are handy tools for impersonating someone's voice and face, being fed enough data; currently we see them used most often in Hollywood productions. In 2022, however, we will see them pop up much more often on our small screens in combination with phishing attacks.

Smishing

COVID-19 facilitated the definitive breakthrough for SMS phishing (smishing, also taking into account web-based texting services). Because many government-associated communication used SMS, for example to inform people of their vaccination codes, hackers started copying these messages and content. They linked these to convincingly spoofed web pages, which led to many accounts of fraud. 2022 will see phishing invent new and unexpected possibilities for a communication tool that is not at all new.





Vishing

When people encounter voice phishing (vishing), they expect it to be a call centre working for Microsoft, telling them there is a problem with their computer. Modern vishing, however, utilises local people, local topics and local sensitivities. It is becoming a lot harder to distinguish real callers from scammers, asking you for your bank account details.

QR code fraud

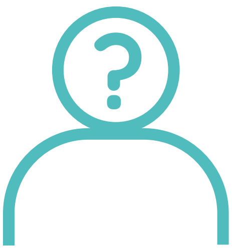
QR codes were invented to broaden the possibilities of the traditional barcode. They have become a popular way to fulfil online transactions, but caution is crucial. A QR code does not show it's intentions right away, which means that scanning one opens the door to possible threats. For instance, hackers can attach extra possibilities when verifying payments so that they gain access to a bank account. Another danger occurs during 'man-in-the-middle' attacks, where a hacker could try to replace a legitimate QR code by his own fraudulent alternative.

Calendar invitations fraud

This re-purposed scam exists in two versions: in one, a hacked entity from a trusted source will send out calendar invitations that bypass spam filters and, in order to be opened, require login information for business 'email) accounts. The entered data is then sent on to the hackers.

In a second version, calendar invites will start filling up your agenda after clicking on a malicious link, pop-up or web banner. Hackers will subsequently contact you to help 'remove the virus', masquerading as a professional cybersecurity firm. In both instances of this scam, be very careful of strange calendar invitations.

Anonymisation



It is becoming easier for attackers to remain anonymous online. This is, in part, due to the rise and popularisation of cryptocurrencies. As a decentralised method of settling accounts, it is increasingly difficult to follow funding streams from point 'A' to point 'B'. Criminals are jumping on the bandwagon and thus placing new barriers between themselves and law enforcement.

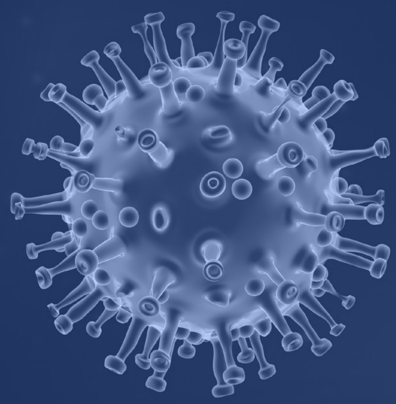
One manifestation of this phenomenon is the breakthrough of 'Bitcoin mules': people who believe to be working for legitimate cryptocurrency agencies, tasked with creating, designating and settling accounts, while in reality they are laundering money which originates from criminal activities.

8. Conclusions

Over 1 in 5 of all employees are at risk of being phished.
When a phishing simulation contains data entry possibilities, 23% of all victims will continue to forfeit their personal information. 7% of all recipients will open possibly malicious attachments.

However, when Phished starts training new clients, we often notice that up to half of all employees within any given organisation will fall into the phishing trap. On average, **45%** will get phished.

The **corona crisis** tops the list in terms of most popular topics and it is clear that this will also be the case in 2022.



The **Omicron variant**, the ongoing vaccination campaigns and the suspicion of health experts that the current crisis could last until at least 2025, create a great responsibility for employers: training people in recognising phishing and help them to handle it safely.

Of course, the other topics should not be forgotten either. Parcel delivery, HR and IT-related topics still sway employees, as do Office-related messages: the influence of **home working** tools is clearly playing its part.

2022 is likely to see a continuation of the trend seen in recent years: phishing will continue to gain **exponentially** in popularity among criminals, which means that cybersecurity awareness providers must remain vigilant.

PHISHED

phished.io hello@phished.io + 44 20 4551 1703