27.10.2021

Omówienie raportu

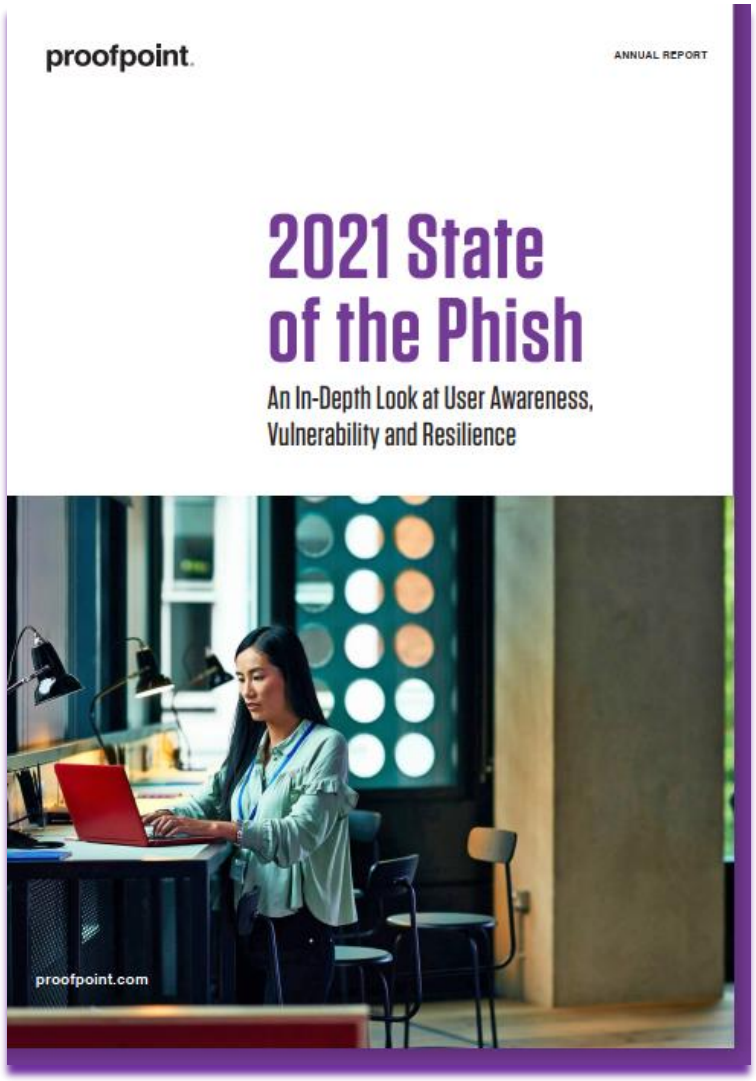
Materiał dla uczestników webinaru „Obowiązki podmiotów z branży Ochrony Zdrowia w ramach Krajowego Systemu Cyberbezpieczeństwa”

2021 State of the Phish

An In-Depth Look at User Awareness, Vulnerability and Resilience

eskom®
IT Outsourcing & Solutions

Czym jest ten raport?

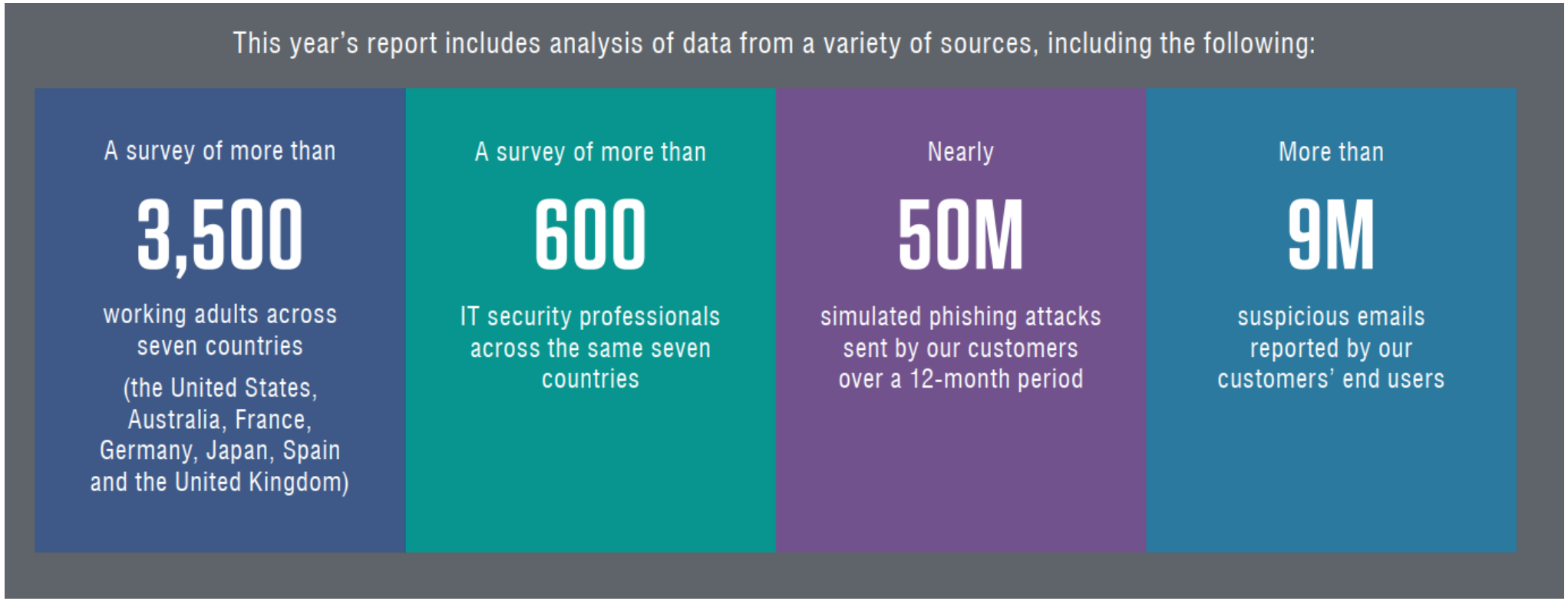


- To jest **coroczny raport** przygotowywany przez firmę – **PROOFPOINT** – lidera w zakresie bezpieczeństwa informacji *[https://www.proofpoint.com/us/company/about]*

- **ESKOM jest partnerem** PROOFPOINT, w zakresie bezpieczeństwa informacji.

Źródło: https://www.proofpoint.com/us/resources/threat-reports/state-of-phish „2021 State of the Phish Report"

Raport bazuje na wielu źródłach.



Źródło: https://www.proofpoint.com/us/resources/threat-reports/state-of-phish „2021 State of the Phish Report"

Czy użytkownicy rozumieją podstawowe zagrożenia?

eskom
IT Outsourcing & Solutions

- Suma odpowiedzi NIEPOPRAWNYCH i „NIE WIEM" np. w przypadku *ransomware* pokazuje, że bardzo duży odsetek >50% nie jest świadoma zagrożenia.
- W przypadku PHISHINGU 4 na 10 użytkowników nie jest świadoma zagrożenia z niego wynikającego.

Źródło: https://www.proofpoint.com/us/resources/threat-reports/state-of-phish „2021 State of the Phish Report"

Smartfony i WIFI 1/2

Smartphones and Wi-Fi: potential weak links

Nearly all survey respondents—95%—said they use a smartphone, and 41% said they use their devices for both personal and work activities. Here's how carefully they protect those devices (see the Appendix for more detail):

- 42% of smartphone owners opt for a biometric lock (such as a fingerprint scan).
- 24% unlock their device using a four-digit PIN.
- 10% have no lock on their device.

Wi-Fi presents another challenge. Open-access networks are virtually everywhere, and device users readily connect (often to avoid data charges). Unfortunately, familiarity can lead to misplaced trust:

- 26% of global respondents think they can safely connect to public Wi-Fi networks in trusted locations, such as local coffee shops and international airports.
- 17% aren't sure whether they should or shouldn't trust open-access Wi-Fi networks in familiar locations.

* Ponad 25% użytkowników smartfonów (smartfonów, na których jest dostęp do danych firmowych) jest przekonanych, że można łączyć się do publicznych, niezabezpieczonych sieci WIFI.

Źródło: https://www.proofpoint.com/us/resources/threat-reports/state-of-phish „2021 State of the Phish Report"

Smartfony i WIFI 2/2

Smartphones and Wi-Fi: potential weak links

But public hotspots aren't the only source of Wi-Fi danger. Working remotely has become more common, which means that home Wi-Fi hygiene can affect the security of your organisation's data and systems.

We found that 95% of global workers have a home Wi-Fi network. But are those networks adequately protected? You be the judge:

- 49% password-protect their network.
- 45% of respondents have personalised the name of their Wi-Fi network.
- 31% have changed the default password on their Wi-Fi router.
- 19% have checked and/or updated their Wi-Fi router's firmware.
- 14% are unsure of how to implement Wi-Fi security measures.
- 11% said they find Wi-Fi security measures too time-consuming and/or inconvenient to implement.

* Mniej niż 50% użytkowników smartfonów (smartfonów, na których jest dostęp do danych firmowych) zabezpiecza hasłem domową sieć WIFI.

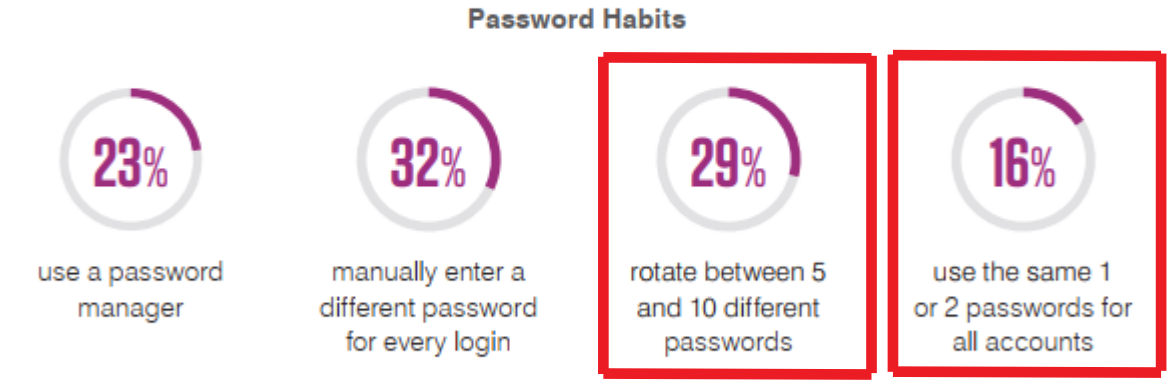
* 2 na 3 użytkowników nie zmieniało domyślnego hasła na ruterze WIFI.

Źródło: https://www.proofpoint.com/us/resources/threat-reports/state-of-phish „2021 State of the Phish Report"

Hasła są re-używane

Passwords and VPNs: misused and misunderstood

Passwords are another source of frustration for infosec and IT teams. Most concerning: users' tendency to reuse passwords. Thankfully, we found that more than half of respondents are avoiding the dreaded practice—but by a slim margin.

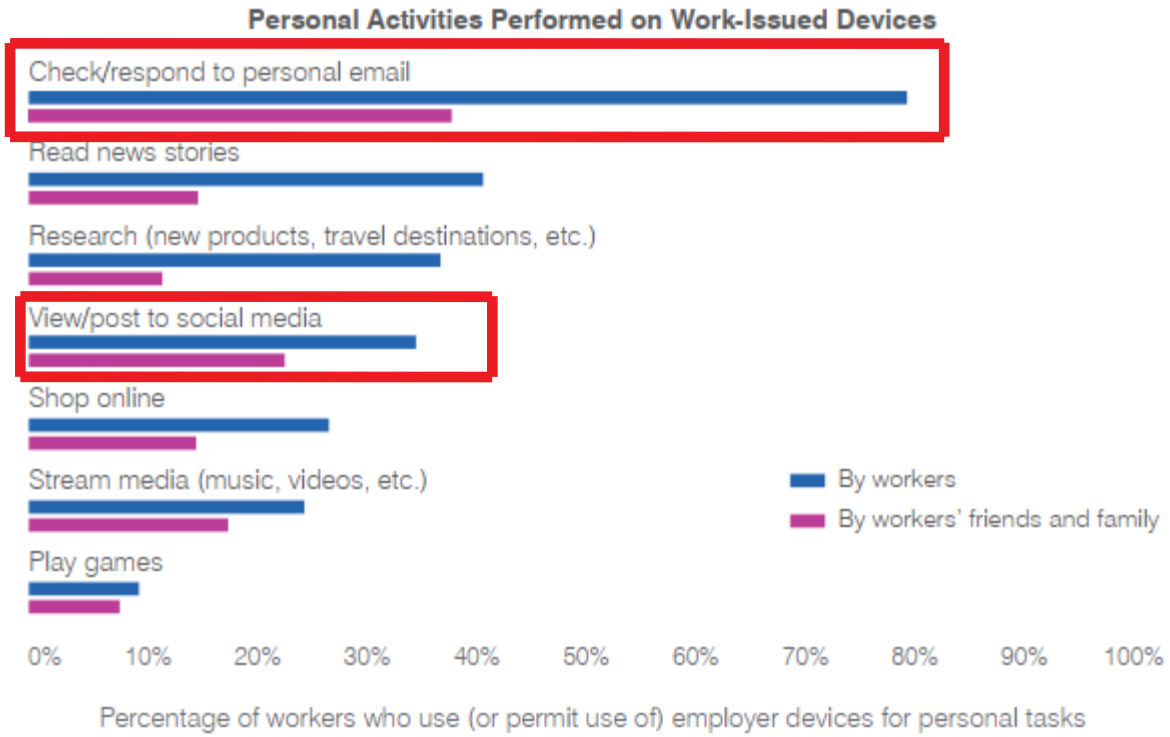


VPNs provide an easy way to protect sensitive data and accounts. Unfortunately, many users—and apparently, the organisations they work for—haven't received the memo.

- Niemal co trzeci użytkownik ma 5 do 10 takich samych haseł, które wykorzystuje we wszystkich serwisach.
- Niemal 2 na 10 użytkowników używa 1 do 2 takich samych haseł do wszystkich serwisów.

Źródło: https://www.proofpoint.com/us/resources/threat-reports/state-of-phish „2021 State of the Phish Report"

Sprzęt służbowy jest powszechnie wykorzystywany prywatnie



KEY FINDING

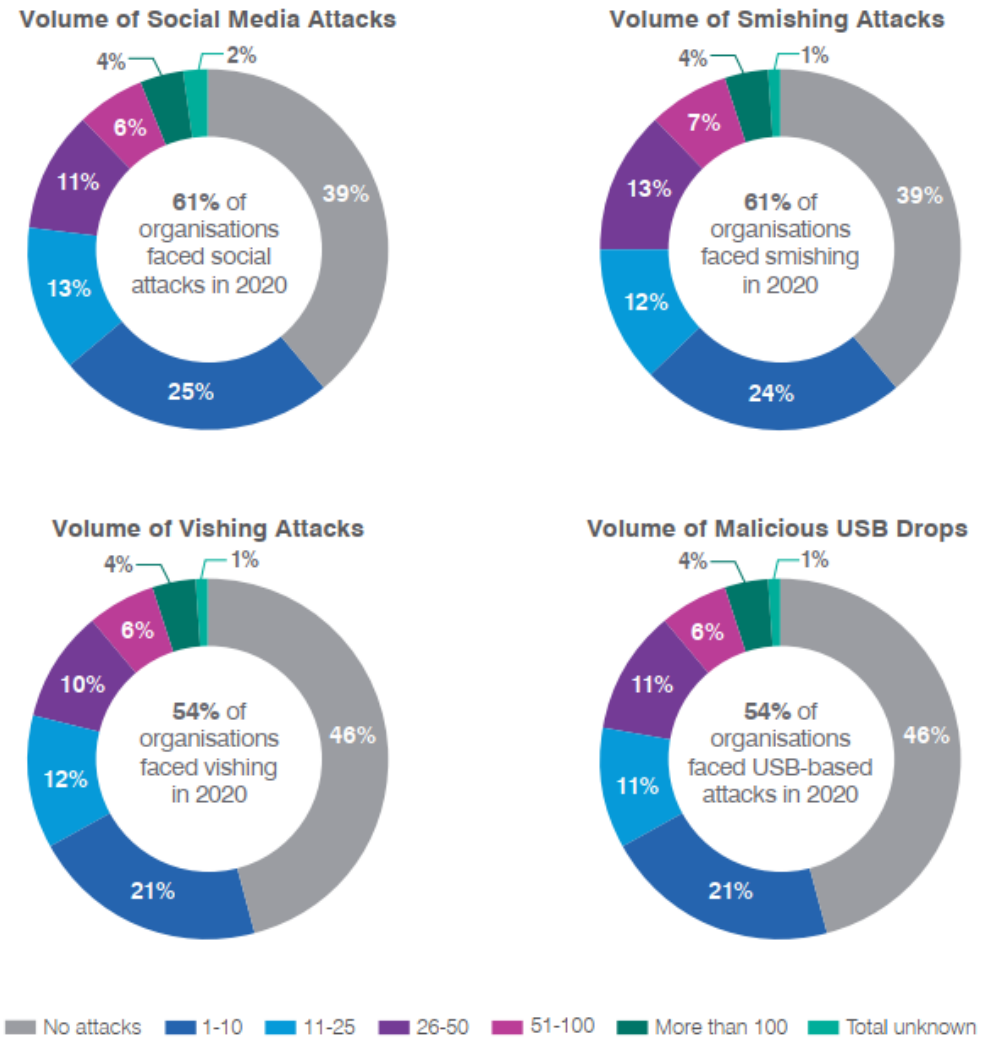
~50%

of respondents said they give friends and family access to their employer-issued devices.

- 80% użytkowników sprawdza prywatną pocztę na służbowym sprzęcie. Połowa z tych użytkowników oddaje sprzęt służbowy innym osobom do korzystania.
- Prawie 40% użytkowników korzysta z kont w serwisach społecznościowych i kupuje online.

Źródło: https://www.proofpoint.com/us/resources/threat-reports/state-of-phish „2021 State of the Phish Report"

Ataki inne, niż z wykorzystaniem maila



- 61% badanych organizacji doświadczyło ataków socjotechnicznych oraz phishingu z wykorzystaniem sms-ów [smishing].
- 54% badanych organizacji doświadczyło ataków z wykorzystaniem phishingu głosowego [vishing] lub wykorzystaniem nośników USB.

Źródło: https://www.proofpoint.com/us/resources/threat-reports/state-of-phish „2021 State of the Phish Report"

Ataki phishingowe: wg rodzajów i skuteczności

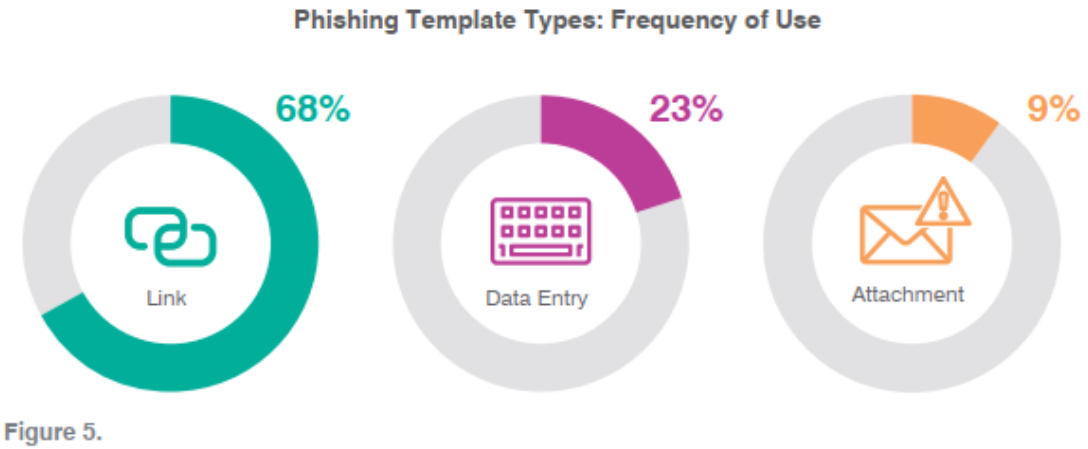


Figure 5.

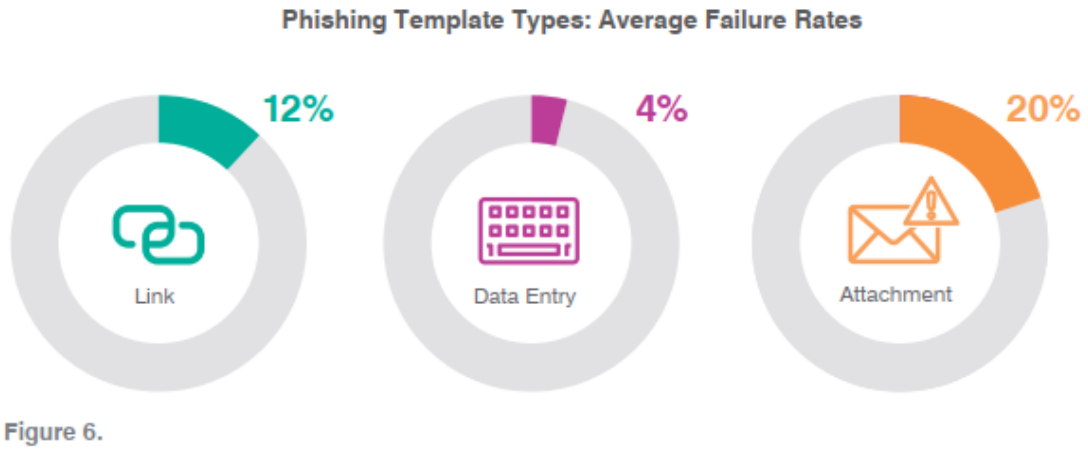


Figure 6.

- **61%** ataków phishingowych oparte było o zainfekowany link, **23%** to ataki polegające na próbie uzyskania haseł i danych do logowania, **9%** to ataki polegające na przesłaniu spreparowanego załącznika.

- *Failure Rate* – wskaźnik w ilu % przypadków użytkownicy **klikali** *lub* **wprowadzali dane** *lub* **uruchamiali złączniki** wynosił odpowiednio 12%, 4% i 20%.

- Choć przesyłanie spreparowanych załączników to **ok. 9%** ataków phishingowych, to co 5 użytkownik uruchamiał taki zainfekowany załącznik.

Źródło: https://www.proofpoint.com/us/resources/threat-reports/state-of-phish „2021 State of the Phish Report"

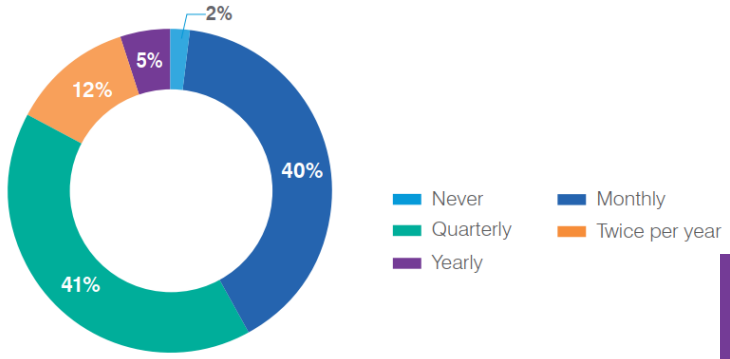
Budowanie świadomości cyber-zagrożeń

Cybersecurity training: are orgs doing enough?

No doubt about it: organisational awareness of cybersecurity education (and the need for it) has risen substantially over the past several years. And in this year's survey of infosec professionals, nearly all said their organisation has a security awareness training programme.

But having a programme is one thing. Running an effective programme is another.

Frequency of Formal Training Sessions



- Świadomość cyber-zagrożeń **to podstawa ograniczania efektów cyber-przestępczości.**
- Prawie wszystkie badane organizacje prowadzą działania w zakresie świadomości cyber-zagrożeń – najczęściej są to szkolenia **– a 2/3 z nich robi to sposób formalny.**

Źródło: https://www.proofpoint.com/us/resources/threat-reports/state-of-phish „2021 State of the Phish Report"

Dziękujemy

ESKOM IT Sp. z o.o.
Puławska 543
02-844 Warszawa
https://www.eskom.eu/

Dział Sprzedaży
+48 22 486 36 63
zapytania@eskom.eu

Inspektor Ochrony Danych Osobowych
iod@eskom.eu

eskom®
IT Outsourcing & Solutions