2024 State of the Phish Report
Key Findings

This document serves as a reference for all country-level statistics and key findings from Proofpoint's 2024 State of the Phish report. Click on the country below to view a full summary of regional findings.

Proofpoint's 2024 State of the Phish Report Findings: GLOBAL

Employees aren't taking risky actions because they lack security awareness: 71% of surveyed working adults admitted to taking risky actions, such as reusing or sharing a password, clicking on links from unknown senders, or handing over their credentials to an untrustworthy source. 96% of them did so knowing the inherent risks involved, meaning that 68% of employees willingly undermined their organization's security. The motivations behind risky actions are varied, with most employees citing convenience (44%), the desire to save time (39%), and a sense of urgency as their main reasons (24%).

Disconnect between IT teams and employees for driving real behavior change: While 85% of surveyed security professionals said that most employees know they are responsible for security, 59% of surveyed employees either weren't sure or claimed that they're not responsible at all. And even though virtually all employees who took a risky action knew the inherent risks—a clear indication security training is working to drive employee awareness—there are clear disparities between what security professionals and employees think is effective to encourage real behavior change. Security pros believe that more training (83%) and tighter controls (81%) are the answer, but nearly all surveyed employees (94%) said they'd prioritize security if controls were simplified and more user-friendly.

MFA continues to provide a false sense of security, leaving businesses exposed: Over one million attacks are launched with the MFA-bypass framework EvilProxy every month, yet, worryingly, 89% of security professionals still believe MFA provides complete protection against account takeover.

Business email compromise (BEC) attacks benefit from AI: Fewer organizations reported email fraud attempts globally, but attack volume grew in countries such as Japan (35% year-over-year increase), South Korea (+31%), and UAE (+29%). These countries may have previously seen fewer BEC attacks due to cultural or language barriers, but generative AI allows attackers to create more convincing and personalized emails in multiple languages. Proofpoint detects an average of 66 million targeted BEC attacks every month.

Cyber extortion persists as lucrative form of attack: 69% of organizations experienced a successful ransomware infection in the past year (a 5-percentage point increase year-over-year); alarmingly, 60% of IT professionals said their organization experienced multiple, separate ransomware infections. Of the organizations impacted by ransomware, 54% agreed to pay attackers (down from 64%), with only 41% regaining access to their data after a single payment (down from 52% a year ago).

Telephone-oriented attack delivery (TOAD) continues to flourish: Although initially appearing as a benign message, containing nothing more than a phone number and some erroneous information, the attack chain is activated when an unsuspecting employee calls a fraudulent call center, providing their credentials or granting remote access to malicious actors. Proofpoint detects 10 million TOAD attacks per month, on average, with a recent peak in August 2023, which drew 13 million incidents.

Despite the growing prominence and sophistication of threats such as ransomware, TOAD and MFA bypass, many organizations are not adequately prepared or trained to deal with them. Only 23% of organizations educate their users on how to recognize and prevent TOAD attacks, and only 23% educate their users on generative AI safety.

Proofpoint's 2024 State of the Phish Report Findings: UK

Phishing data for subhead and para 1: And while the incidence of successful phishing attacks has slightly declined (66% of surveyed organizations experienced at least one successful attack in 2023 versus 91% the previous year), the negative consequences have soared: a 30% increase in reports of financial penalties, such as regulatory fines, and a 78% increase in reports of reputational damage.

Employees aren't taking risky actions because they lack security awareness: 70% of surveyed working adults admitted to taking risky actions, such as reusing or sharing a password, clicking on links from unknown senders, or handing over their credentials to an untrustworthy source. 95% of them did so knowing the inherent risks involved, meaning that 67% of UK employees willingly undermined their organization's security. The motivations behind risky actions are varied, with most employees citing convenience (48%), the desire to save time (40%), and a sense of urgency as their main reasons (22%).

Disconnect between IT teams and employees for driving real behavior change: While 81% of surveyed security professionals said that most employees know they are responsible for security, 58% of surveyed employees either weren't sure or claimed that they're not responsible at all. And even though virtually all employees who took a risky action knew the inherent risks (96%) —a clear indication security training is working to drive employee awareness—there are clear disparities between what security professionals and employees think is effective to encourage real behavior change. Security pros believe that more training (85%) and tighter controls (89%) are the answer, but nearly all surveyed employees (94%) said they'd prioritize security if controls were simplified and more user-friendly.

MFA continues to provide a false sense of security, leaving businesses exposed: Over one million attacks are launched with the MFA-bypass framework EvilProxy every month, yet, worryingly, 92% of UK security professionals still believe MFA provides complete protection against account takeover.

Business email compromise (BEC) attacks benefit from AI: In the UK, 74% of organisations were targeted by BEC attacks in 2023, compared to 86% in 2022. Overall, fewer organisations reported email fraud attempts globally, but attack volume grew in countries such as Japan (35% year-over-year increase), South Korea (+31%), and the UAE (+29%). These countries may have previously seen fewer BEC attacks due to cultural or language barriers, but generative AI allows attackers to create more convincing and personalized emails in multiple languages. Proofpoint detects an average of 66 million targeted BEC attacks every month.

Cyber extortion persists as lucrative form of attack: 64% of UK organizations experienced a successful ransomware infection in the past year (a 3-percentage point increase year-over-year); alarmingly, 77% of UK IT professionals said their organization experienced multiple, separate ransomware infections. Of the organizations impacted by ransomware, 64% agreed to pay attackers (up from 63%), with only 34% regaining access to their data after a single payment (up from 33% a year ago).

Telephone-oriented attack delivery (TOAD) continues to flourish: Although initially appearing as a benign message, containing nothing more than a phone number and some erroneous information, the attack chain is activated when an unsuspecting employee calls a fraudulent call center, providing their credentials or granting remote access to malicious actors. Proofpoint detects 10 million TOAD attacks per month, on average, with a recent peak in August 2023, which drew 13 million incidents.

Despite the growing prominence and sophistication of threats such as ransomware, TOAD and MFA bypass, many organisations are not adequately prepared or trained to deal with them. Only 28% of UK organizations educate their users on how to recognize and prevent TOAD attacks, and only 26% educate their users on generative AI safety.

Proofpoint's 2024 State of the Phish Report Findings: FRANCE

Phishing data for subhead and para 1: And while the incidence of successful phishing attacks has slightly declined (66% of surveyed organizations in France experienced at least one successful attack in 2023 versus 86% the previous year), the negative consequences have soared: a 320% increase in reports of financial penalties, such as regulatory fines, and a 166% increase in reports of reputational damage. Other consequences for organisations in France included widespread network outage and downtime (32%), loss of organizational data (30%) and credential breach/account compromise (27%).

Employees aren't taking risky actions because they lack security awareness: 79% of surveyed working adults admitted to taking risky actions, such as reusing or sharing a password, clicking on links from unknown senders, or handing over their credentials to an untrustworthy source. 95% of them did so knowing the inherent risks involved, meaning that 75% of French employees willingly undermined their organization's security. The motivations behind risky actions are varied, with most employees citing convenience (43%), the desire to save time (36%), and a sense of urgency as their main reasons (29%).

Disconnect between IT teams and employees for driving real behavior change: While 79% of surveyed security professionals said that most employees know they are responsible for security, 64% of surveyed employees either weren't sure or claimed that they're not responsible at all. And even though virtually all employees who took a risky action knew the inherent risks (95%) —a clear indication security training is working to drive employee awareness—there are clear disparities between what security professionals and employees think is effective to encourage real behavior change. Security pros believe that more training (76%) and tighter controls (80%) are the answer, but nearly all surveyed employees (94%) said they'd prioritize security if controls were simplified and more user-friendly.

MFA continues to provide a false sense of security, leaving businesses exposed: Over one million attacks are launched with the MFA-bypass framework EvilProxy every month, yet, worryingly, 91% of French security professionals still believe MFA provides complete protection against account takeover.

Business email compromise (BEC) attacks benefit from AI: In France, 62% of organisations were targeted by BEC attacks in 2023, compared to 80% in 2022. Overall, fewer organisations reported email fraud attempts globally, but attack volume grew in countries such as Japan (35% year-over-year increase), South Korea (+31%), and the UAE (+29%). These countries may have previously seen fewer BEC attacks due to cultural or language barriers, but generative AI allows attackers to create more convincing and personalized emails in multiple languages. Proofpoint detects an average of 66 million targeted BEC attacks every month.

Cyber extortion persists as lucrative form of attack: 70% of French organizations experienced a successful ransomware infection in the past year (a 6-percentage point increase year-over-year); alarmingly, 63% of French IT professionals said their organization experienced multiple, separate ransomware infections. Of the organizations impacted by ransomware, 30% agreed to pay attackers (down from 53%), with only 47% regaining access to their data after a single payment (down from 63% a year ago).

Telephone-oriented attack delivery (TOAD) continues to flourish: Although initially appearing as a benign message, containing nothing more than a phone number and some erroneous information, the attack chain is activated when an unsuspecting employee calls a fraudulent call centre, providing their credentials or granting remote access to malicious actors. Proofpoint detects 10 million TOAD attacks per month, on average, with a recent peak in August 2023, which drew 13 million incidents.

Despite the growing prominence and sophistication of threats such as ransomware, TOAD and MFA bypass, many organisations are not adequately prepared or trained to deal with them. Only 16% of

French organisations educate their users on how to recognize and prevent TOAD attacks, and only 25% educate their users on generative AI safety.

Proofpoint's 2024 State of the Phish Report Findings: GERMANY

Phishing data for subhead and para 1: And while the incidence of successful phishing attacks has slightly declined (86% of surveyed organizations in Germany experienced at least one successful attack in 2023 versus 89% the previous year), the negative consequences have soared: a 500% increase in reports of financial penalties, such as regulatory fines, and a 67% increase in reports of reputational damage.

Employees aren't taking risky actions because they lack security awareness: 69% of surveyed working adults admitted to taking risky actions, such as reusing or sharing a password, clicking on links from unknown senders, or handing over their credentials to an untrustworthy source. 93% of them did so knowing the inherent risks involved, meaning that 64% of German employees willingly undermined their organization's security. The motivations behind risky actions are varied, with most employees citing convenience (46%), the desire to save time (44%), and a sense of urgency as their main reasons (22%).

Disconnect between IT teams and employees for driving real behavior change: While 86% of surveyed security professionals said that most employees know they are responsible for security, 65% of surveyed employees either weren't sure or claimed that they're not responsible at all. And even though virtually all employees who took a risky action knew the inherent risks (93%) —a clear indication security training is working to drive employee awareness—there are clear disparities between what security professionals and employees think is effective to encourage real behavior change. Security pros believe that more training (80%) and tighter controls (92%) are the answer, but nearly all surveyed employees (92%) said they'd prioritize security if controls were simplified and more user-friendly.

MFA continues to provide a false sense of security, leaving businesses exposed: Over one million attacks are launched with the MFA-bypass framework EvilProxy every month, yet, worryingly, 89% of German security professionals still believe MFA provides complete protection against account takeover.

Business email compromise (BEC) attacks benefit from AI: In Germany, 82% of organisations were targeted by BEC attacks in 2023, compared to 86% in 2022. Overall, fewer organisations reported email fraud attempts globally, but attack volume grew in countries such as Japan (35% year-over-year increase), South Korea (+31%), and the UAE (+29%). These countries may have previously seen fewer BEC attacks due to cultural or language barriers, but generative AI allows attackers to create more convincing and personalized emails in multiple languages. Proofpoint detects an average of 66 million targeted BEC attacks every month.

Cyber extortion persists as lucrative form of attack: 85% of German organizations experienced a successful ransomware infection in the past year (a 35% increase year-over-year); alarmingly, 75% of German IT professionals said their organization experienced multiple, separate ransomware infections. Of the organizations impacted by ransomware, almost all (93%) agreed to pay attackers (up from 81%) with 63% regaining access to their data after a single payment (up from 41% a year ago).

Telephone-oriented attack delivery (TOAD) continues to flourish: Although initially appearing as a benign message, containing nothing more than a phone number and some erroneous information, the attack chain is activated when an unsuspecting employee calls a fraudulent call centre, providing their credentials or granting remote access to malicious actors. Proofpoint detects 10 million TOAD attacks per month, on average, with a recent peak in August 2023, which drew 13 million incidents.

Despite the growing prominence and sophistication of threats such as ransomware, TOAD and MFA bypass, many organisations are not adequately prepared or trained to deal with them. Only 21% of German organisations educate their users on how to recognize and prevent TOAD attacks, and equally only 21% educate their users on generative AI safety.

Proofpoint's 2024 State of the Phish Report Findings: ITALY

Phishing data for subhead and para 1: And while the incidence of successful phishing attacks has slightly declined (65% of surveyed organizations in Italy experienced at least one successful attack in 2023 versus 79% the previous year), the negative consequences have soared: a 100% increase in reports of financial penalties, such as regulatory fines, and a 385% increase in reports of reputational damage.

Employees aren't taking risky actions because they lack security awareness: 74% of surveyed working adults admitted to taking risky actions, such as reusing or sharing a password, clicking on links from unknown senders, or handing over their credentials to an untrustworthy source. 97% of them did so knowing the inherent risks involved, meaning that 72% of Italian employees willingly undermined their organization's security. The motivations behind risky actions are varied, with most employees citing convenience (34%), the desire to save time (41%), and a sense of urgency as their main reasons (24%).

Disconnect between IT teams and employees for driving real behavior change: While 74% of surveyed security professionals said that most employees know they are responsible for security, 63% of surveyed employees either weren't sure or claimed that they're not responsible at all. And even though virtually all employees who took a risky action knew the inherent risks (97%) —a clear indication security training is working to drive employee awareness—there are clear disparities between what security professionals and employees think is effective to encourage real behavior change. Security pros believe that more training (82%) and tighter controls (78%) are the answer, but nearly all surveyed employees (93%) said they'd prioritize security if controls were simplified and more user-friendly.

MFA continues to provide a false sense of security, leaving businesses exposed: Over one million attacks are launched with the MFA-bypass framework EvilProxy every month, yet, worryingly, 89% of Italian security professionals still believe MFA provides complete protection against account takeover.

Business email compromise (BEC) attacks benefit from AI: In Italy, 51% of organisations were targeted by BEC attacks in 2023 (the same % as 2022). Overall, fewer organisations reported email fraud attempts globally, but attack volume grew in countries such as Japan (35% year-over-year increase), South Korea (+31%), and the UAE (+29%). These countries may have previously seen fewer BEC attacks due to cultural or language barriers, but generative AI allows attackers to create more convincing and personalized emails in multiple languages. Proofpoint detects an average of 66 million targeted BEC attacks every month.

Cyber extortion persists as lucrative form of attack: 71% of Italian organizations experienced a successful ransomware infection in the past year (a 61% increase year-over-year); alarmingly, 66% of Italian IT professionals said their organization experienced multiple, separate ransomware infections. Of the organizations impacted by ransomware, 23% agreed to pay attackers (down from 27%) with only 25% regaining access to their data after a single payment (down from 38% a year ago).

Telephone-oriented attack delivery (TOAD) continues to flourish: Although initially appearing as a benign message, containing nothing more than a phone number and some erroneous information, the attack chain is activated when an unsuspecting employee calls a fraudulent call centre, providing their credentials or granting remote access to malicious actors. Proofpoint detects 10 million TOAD attacks per month, on average, with a recent peak in August 2023, which drew 13 million incidents.

Despite the growing prominence and sophistication of threats such as ransomware, TOAD and MFA bypass, many organisations are not adequately prepared or trained to deal with them. Only 23% of Italian organisations educate their users on how to recognize and prevent TOAD attacks, and equally only 15% educate their users on generative AI safety.

Proofpoint's 2024 State of the Phish Report Findings: SPAIN

Phishing data for subhead and para 1: And while the incidence of successful phishing attacks has slightly declined (67% of surveyed organizations in Spain experienced at least one successful attack in 2023 versus 90% the previous year), the negative consequences have soared: a 25% increase in reports of financial penalties, such as regulatory fines, and a 56% increase in reports of reputational damage.

Employees aren't taking risky actions because they lack security awareness: 73% of surveyed working adults admitted to taking risky actions, such as reusing or sharing a password, clicking on links from unknown senders, or handing over their credentials to an untrustworthy source. 94% of them did so knowing the inherent risks involved, meaning that 67% of Spanish employees willingly undermined their organization's security. The motivations behind risky actions are varied, with most employees citing convenience (27%), the desire to save time (42%), and a sense of urgency as their main reasons (25%).

Disconnect between IT teams and employees for driving real behavior change: While 86% of surveyed security professionals said that most employees know they are responsible for security, 55% of surveyed employees either weren't sure or claimed that they're not responsible at all. And even though virtually all employees who took a risky action knew the inherent risks (94%) —a clear indication security training is working to drive employee awareness—there are clear disparities between what security professionals and employees think is effective to encourage real behavior change. Security pros believe that more training (83%) and tighter controls (84%) are the answer, but nearly all surveyed employees (95%) said they'd prioritize security if controls were simplified and more user-friendly.

MFA continues to provide a false sense of security, leaving businesses exposed: Over one million attacks are launched with the MFA-bypass framework EvilProxy every month, yet, worryingly, 84% of Spanish security professionals still believe MFA provides complete protection against account takeover.

Business email compromise (BEC) attacks benefit from AI: In Spain, 70% of organisations were targeted by BEC attacks in 2023 (compared to 90% in 2022). Overall, fewer organisations reported email fraud attempts globally, but attack volume grew in countries such as Japan (35% year-over-year increase), South Korea (+31%), and the UAE (+29%). These countries may have previously seen fewer BEC attacks due to cultural or language barriers, but generative AI allows attackers to create more convincing and personalized emails in multiple languages. Proofpoint detects an average of 66 million targeted BEC attacks every month.

Cyber extortion persists as lucrative form of attack: 69% of Spanish organizations experienced a successful ransomware infection in the past year (72% in 2022); alarmingly, 55% of Spanish IT professionals said their organization experienced multiple, separate ransomware infections. Of the organizations impacted by ransomware, 42% agreed to pay attackers (down from 64%) with only 21% regaining access to their data after a single payment (down from 50% a year ago).

Telephone-oriented attack delivery (TOAD) continues to flourish: Although initially appearing as a benign message, containing nothing more than a phone number and some erroneous information, the attack chain is activated when an unsuspecting employee calls a fraudulent call centre, providing their credentials or granting remote access to malicious actors. Proofpoint detects 10 million TOAD attacks per month, on average, with a recent peak in August 2023, which drew 13 million incidents.

Despite the growing prominence and sophistication of threats such as ransomware, TOAD and MFA bypass, many organisations are not adequately prepared or trained to deal with them. Only 28% of Spanish organisations educate their users on how to recognize and prevent TOAD attacks, and only 20% educate their users on generative AI safety.

Proofpoint's 2024 State of the Phish Report Findings: SWEDEN

Phishing data for subhead and para 1: And while the incidence of successful phishing attacks has slightly declined (72% of surveyed organizations in Sweden experienced at least one successful attack in 2023 versus 94% the previous year), the negative consequences have soared: a 167% increase in reports of financial penalties, such as regulatory fines, and a 30% increase in reports of reputational damage.

Employees aren't taking risky actions because they lack security awareness: 82% of surveyed working adults admitted to taking risky actions, such as reusing or sharing a password, clicking on links from unknown senders, or handing over their credentials to an untrustworthy source. 94% of them did so knowing the inherent risks involved, meaning that 77% of Swedish employees willingly undermined their organization's security. The motivations behind risky actions are varied, with most employees citing convenience (37%), the desire to save time (46%), and a sense of urgency as their main reasons (22%).

Disconnect between IT teams and employees for driving real behavior change: While 84% of surveyed security professionals said that most employees know they are responsible for security, 66% of surveyed employees either weren't sure or claimed that they're not responsible at all. And even though virtually all employees who took a risky action knew the inherent risks (94%) —a clear indication security training is working to drive employee awareness—there are clear disparities between what security professionals and employees think is effective to encourage real behavior change. Security pros believe that more training (78%) and tighter controls (67%) are the answer, but nearly all surveyed employees (93%) said they'd prioritize security if controls were simplified and more user-friendly.

MFA continues to provide a false sense of security, leaving businesses exposed: Over one million attacks are launched with the MFA-bypass framework EvilProxy every month, yet, worryingly, 84% of Swedish security professionals still believe MFA provides complete protection against account takeover.

Business email compromise (BEC) attacks benefit from AI: In Sweden, 92% of organisations were targeted by BEC attacks in 2023 (same % as 2022). Overall, fewer organisations reported email fraud attempts globally, but attack volume grew in countries such as Japan (35% year-over-year increase), South Korea (+31%), and the UAE (+29%). These countries may have previously seen fewer BEC attacks due to cultural or language barriers, but generative AI allows attackers to create more convincing and personalized emails in multiple languages. Proofpoint detects an average of 66 million targeted BEC attacks every month.

Cyber extortion persists as lucrative form of attack: 66% of Swedish organizations experienced a successful ransomware infection in the past year (down from 82% in 2022); alarmingly, 63% of Swedish IT professionals said their organization experienced multiple, separate ransomware infections. Of the organizations impacted by ransomware, 60% agreed to pay attackers (down from 80%) with only 21% regaining access to their data after a single payment (down from 52% a year ago).

Telephone-oriented attack delivery (TOAD) continues to flourish: Although initially appearing as a benign message, containing nothing more than a phone number and some erroneous information, the attack chain is activated when an unsuspecting employee calls a fraudulent call centre, providing their

credentials or granting remote access to malicious actors. Proofpoint detects 10 million TOAD attacks per month, on average, with a recent peak in August 2023, which drew 13 million incidents.

Despite the growing prominence and sophistication of threats such as ransomware, TOAD and MFA bypass, many organisations are not adequately prepared or trained to deal with them. Only 22% of Swedish organisations educate their users on how to recognize and prevent TOAD attacks, and equally only 22% educate their users on generative AI safety.

Proofpoint's 2024 State of the Phish Report Findings: THE NETHERLANDS

Phishing data for subhead and para 1: And while the incidence of successful phishing attacks has slightly declined (84% of surveyed organizations in the Netherlands experienced at least one successful attack in 2023 versus 90% the previous year), the negative consequences have soared: a 460% increase in reports of financial penalties, such as regulatory fines.

Employees aren't taking risky actions because they lack security awareness: 73% of surveyed working adults admitted to taking risky actions, such as reusing or sharing a password, clicking on links from unknown senders, or handing over their credentials to an untrustworthy source. 95% of them did so knowing the inherent risks involved, meaning that 69% of Dutch employees willingly undermined their organization's security. The motivations behind risky actions are varied, with most employees citing convenience (47%), the desire to save time (32%), and a sense of urgency as their main reasons (15%).

Disconnect between IT teams and employees for driving real behavior change: While 84% of surveyed security professionals said that most employees know they are responsible for security, 66% of surveyed employees either weren't sure or claimed that they're not responsible at all. And even though virtually all employees who took a risky action knew the inherent risks (95%) —a clear indication security training is working to drive employee awareness—there are clear disparities between what security professionals and employees think is effective to encourage real behavior change. Security pros believe that more training (87%) and tighter controls (74%) are the answer, but nearly all surveyed employees (96%) said they'd prioritize security if controls were simplified and more user-friendly.

MFA continues to provide a false sense of security, leaving businesses exposed: Over one million attacks are launched with the MFA-bypass framework EvilProxy every month, yet, worryingly, 82% of Dutch security professionals still believe MFA provides complete protection against account takeover.

Business email compromise (BEC) attacks benefit from AI: In the Netherlands, 76% of organisations were targeted by BEC attacks in 2023 (down from 92% in 2022). Overall, fewer organisations reported email fraud attempts globally, but attack volume grew in countries such as Japan (35% year-over-year increase), South Korea (+31%), and the UAE (+29%). These countries may have previously seen fewer BEC attacks due to cultural or language barriers, but generative AI allows attackers to create more convincing and personalized emails in multiple languages. Proofpoint detects an average of 66 million targeted BEC attacks every month.

Cyber extortion persists as lucrative form of attack: 72% of Dutch organizations experienced a successful ransomware infection in the past year (down from 76% in 2022); alarmingly, 50% of Dutch IT professionals said their organization experienced multiple, separate ransomware infections. Of the organizations impacted by ransomware, 56% agreed to pay attackers (down from 76%) with only 25% regaining access to their data after a single payment (down from 52% a year ago).

Telephone-oriented attack delivery (TOAD) continues to flourish: Although initially appearing as a benign message, containing nothing more than a phone number and some erroneous information, the attack chain is activated when an unsuspecting employee calls a fraudulent call centre, providing their

credentials or granting remote access to malicious actors. Proofpoint detects 10 million TOAD attacks per month, on average, with a recent peak in August 2023, which drew 13 million incidents.

Despite the growing prominence and sophistication of threats such as ransomware, TOAD and MFA bypass, many organisations are not adequately prepared or trained to deal with them. Only 32% of Dutch organisations educate their users on how to recognize and prevent TOAD attacks, and only 18% educate their users on generative AI safety.

Proofpoint's 2024 State of the Phish Report Findings: UAE

Phishing data for subhead and para 1: And while the incidence of successful phishing attacks has slightly declined globally, in the UAE it is on the rise (92% of surveyed organizations in the UAE experienced at least one successful attack in 2023 versus 86% the previous year), the negative consequences have also soared: a 44% increase in reports of financial penalties, such as regulatory fines, and a 300% increase in reports of reputational damage.

Employees aren't taking risky actions because they lack security awareness: 86% of surveyed working adults admitted to taking risky actions, such as reusing or sharing a password, clicking on links from unknown senders, or handing over their credentials to an untrustworthy source. 97% of them did so knowing the inherent risks involved, meaning that 83% of UAE employees willingly undermined their organization's security. The motivations behind risky actions are varied, with most employees citing convenience (32%), the desire to save time (46%), and a sense of urgency as their main reasons (31%).

Disconnect between IT teams and employees for driving real behavior change: While 90% of surveyed security professionals said that most employees know they are responsible for security, 38% of surveyed employees either weren't sure or claimed that they're not responsible at all. And even though virtually all employees who took a risky action knew the inherent risks (97%) —a clear indication security training is working to drive employee awareness—there are clear disparities between what security professionals and employees think is effective to encourage real behavior change. Security pros believe that more training (90%) and tighter controls (92%) are the answer, but nearly all surveyed employees (94%) said they'd prioritize security if controls were simplified and more user-friendly.

MFA continues to provide a false sense of security, leaving businesses exposed: Over one million attacks are launched with the MFA-bypass framework EvilProxy every month, yet, worryingly, 94% of UAE security professionals still believe MFA provides complete protection against account takeover.

Business email compromise (BEC) attacks benefit from AI: In the UAE, 85% of organisations were targeted by BEC attacks in 2023 (up from 66% in 2022). Overall, fewer organisations reported email fraud attempts globally, but attack volume grew in countries such as Japan (35% year-over-year increase), South Korea (+31%), and the UAE (+29%). These countries may have previously seen fewer BEC attacks due to cultural or language barriers, but generative AI allows attackers to create more convincing and personalized emails in multiple languages. Proofpoint detects an average of 66 million targeted BEC attacks every month.

Cyber extortion persists as lucrative form of attack: 77% of UAE organizations experienced a successful ransomware infection in the past year (up from 70% in 2022); alarmingly, 66% of UAE IT professionals said their organization experienced multiple, separate ransomware infections. Of the organizations impacted by ransomware, 80% agreed to pay attackers (up from 66%) with 66% regaining access to their data after a single payment (up from 61% a year ago).

Telephone-oriented attack delivery (TOAD) continues to flourish: Although initially appearing as a benign message, containing nothing more than a phone number and some erroneous information, the attack chain is activated when an unsuspecting employee calls a fraudulent call centre, providing their credentials or granting remote access to malicious actors. Proofpoint detects 10 million TOAD attacks per month, on average, with a recent peak in August 2023, which drew 13 million incidents.

Despite the growing prominence and sophistication of threats such as ransomware, TOAD and MFA bypass, many organisations are not adequately prepared or trained to deal with them. Only 13% of UAE organisations educate their users on how to recognize and prevent TOAD attacks, and only 21% educate their users on generative AI safety.