**Cyberbezpieczeństwo w firmie. Jak zainteresować pracowników tym tematem?**

**Czy wiesz, że poczta e-mail wciąż jest głównym wektorem cyberataków? Klikanie w podejrzane linki i odwiedzanie zainfekowanych stron to pięta achillesowa większości z nas. Przez ostatnie trzy lata niewiele się w tej kwestii zmieniło, prawnie 60% osób daje się nabrać na triki cyberprzestępców. Jeśli chcesz chronić swój biznes, musisz edukować pracowników. Poniżej znajdziesz kilka pomysłów na to, jak szerzyć wiedzę o cyberbezpieczeństwie w firmie nie wydając ani złotówki.**

Poczta e-mail wciąż jest głównym wektorem cyberataków – czytamy w CISO Benchmark Study 2019. Tak, Twoi pracownicy najprawdopodobniej klikają w podejrzane linki i odwiedzają zainfekowane strony. Przez ostatnie trzy lata niewiele się w tej kwestii zmieniło, prawnie 60% osób daje się oszukać cyberprzestępcom. Niby mówi się o tym coraz więcej, zwłaszcza że atakujący nierzadko mistrzowsko podszywają się pod zaufane instytucje, a jednak wiedza ta odbija się jak przysłowiowy groch o ścianę.

Co robić? Złożyć broń? Niekoniecznie. Jeśli chcesz bronić swój biznes, podaruj tarcze swoim pracownikom. Wyposaż ich w wiedzę. Edukacja nic nie kosztuje, a ma większy wpływ na ochronę Twojej firmy przed cyberatakami niż najlepszy firewall czy program antywirusowy.

Interaktywny quiz z nagrodami

Nauka przez zabawę? Sprawdź wiedzę związaną z bezpieczeństwem w Internecie swoich pracowników zapraszając ich do… udziału w quizie.

Taki quiz ma kilka zastosowań: po pierwsze pracownicy poznają potencjalne zagrożenia. W przyszłości – jeśli znajdą się w podobnej sytuacji – z pewnością zastanowią się dwa razy, zanim klikną w jakiś podejrzany link albo pominą ważne aktualizacje.

Po drugie: dowiesz się, które zagadnienia dotyczące cyberbezpieczeństwa wymagają rozwinięcia i doprecyzowania w Twojej firmie.

Po trzecie: to doskonały sposób na szybką integrację. Dla specjalnego efektu dorzuć drobną nagrodę dla najlepszych, choćby w postaci słodkości.

Quiz możesz zrobić tu: <https://testbezpieczenstwa.specfile.pl/quiz>

Darmowy audyt bezpieczeństwa

Phishingu czyli próba wyłudzenia wrażliwych danych, uzyskania dostępu do Twojego komputera lub zainfekowania go udaje się cyberprzestępcom częściej niż myślisz. Ponad 90% ataków wykonywanych jest właśnie prze e-mail. Przestępcy używają coraz bardziej wyrafinowanych metod, by Twój pracownik dał się nabrać na ten stary trik: kliknął w podany w wiadomości link.

Na szczęście możesz sprawdzić podatność na cyberataki zlecając bezpłatny audyt bezpieczeństwa. Wystarczy, że wskażesz emaile pracowników. Otrzymasz raport z audytu i dowiesz się czy Twoja firma jest bezpieczna. A ponieważ cały ten proceder ma za zadanie edukować, koniecznie wyróżnij osoby, które są odporne na pokusy klikania. To dobry sposób, by rozpocząć z pracownikami rozmowę o tym zjawisku i socjotechnikach stosowanych przez cyberprzestępców.

Zleć bezpłatny audyt tutaj: https://testbezpieczenstwa.specfile.pl/

Szkolenia nie zawsze są płatne

Możliwości jest coraz więcej: webinaria, kursy, szkolenia. Nie musisz się obawiać, że wydasz na edukację pracowników majątek, ponieważ wiele takich spotkań jest bezpłatnych. Szczególnie warto przejrzeć ofertę ośrodków dydaktyczno-szkoleniowych przy urzędzie w Twoim mieście.