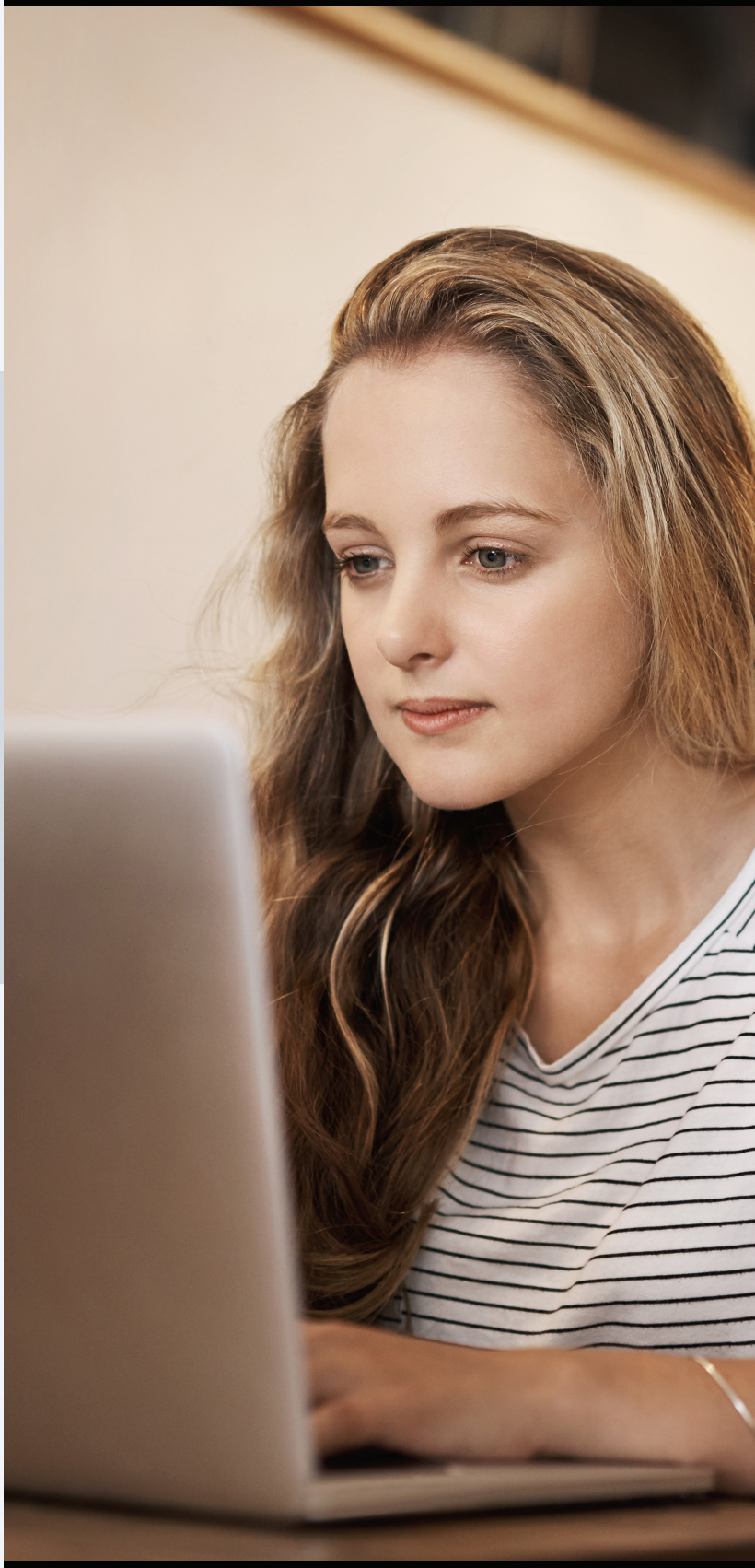
Wzmacniamypierwszą linię obrony i najsłabsze ogniwo: człowieka.

IBM Security



Świetnym sposobem ochrony firmy przez pracowników jest... nieotwieranie przez nich żadnych wiadomości e-mail. Jeszcze lepszym rozwiązaniem będzie jednak zapewnienie personelowi odpowiedniego przeszkolenia.

Usługi IBM w zakresie uświadamiania i szkoleń w dziedzinie bezpieczeństwa

Zespół IBM Security oferuje kompleksowy program rozwoju i ciągłego wdrażania szkoleń i działań uświadamiających pracowników na temat phishingu. Ma on na celu stworzenie i pielęgnowanie kultury pracy nacechowanej świadomością ryzyka. Taki specjalnie dostosowany i opracowany z myślą o nieustannym wdrażaniu program uświadamiający proponujemy także i Twojej organizacji.

Phishing pozostaje jednym z najbardziej istotnych źródeł zagrożeń, a nasze usługi pomagają pracownikom w lepszym przygotowaniu się na próby jego wykorzystania i ataki socjotechniczne. Szkoląc pracowników naszych klientów, korzystamy z rozwiązań e-learningowych, gamifikacji, symulacji ataków phishingowych i socjotechnicznych. Nasi doświadczeni konsultanci dbają o dostosowanie platformy i metod szkolenia do indywidualnych potrzeb klienta, zapewniają potrzebne wskaźniki, raportowanie i zarządzanie programem.

Rozpocznij już dzisiaj

Dowiedz się więcej o korzyściach naszego Programu uświadamiania i szkoleń w zakresie bezpieczeństwa.

Skontaktuj się z zespołem IBM ds. usług w dziedzinie bezpieczeństwa:
ibm.biz/BdqYUF.

IBM

Kompleksowy program uświadamiania i szkoleń w zakresie bezpieczeństwa może pomóc w minimalizacji ryzyka dla organizacji.

Na opracowanie programu składa się pięć kroków.

1. Zdefiniowanie

- **Zdefiniowanie celów programu**
- **Zdefiniowanie odbiorców docelowych (zakres)**
- **Zdefiniowanie wskaźników KPI**
- **Zdefiniowanie wymagań dla programu i wymogów w zakresie zgodności z przepisami**

2. Ustalenie

- **Ustalenie ram uświadamianej wiedzy na temat cyberbezpieczeństwa**
- **Utworzenie planu budowania świadomości**
- **Utworzenie artefaktów i instrukcji szkoleniowych**
- **Pozyskanie wsparcia zarządu**

3. Ocena

- **Ocena aktualnego stanu wiedzy na temat bezpieczeństwa informacji**
- **Ocena aktualnego rozumienia przez pracowników powierzonych im ról oraz ich zdolności do ochrony bezpieczeństwa informacji**

4. Wdrożenie

- **Przeprowadzenie niezbędnych prac integracyjnych i dostosowawczych**
- **Przeprowadzenie szkoleń, kampanii, quizów i ankiet**
- **Aktywacja konta do szkoleń komputerowych**

5. Pomiar

- **Śledzenie i pomiar skuteczności programu**
- **Raportowanie ocen i przebiegu szkolenia**
- **Opracowanie wyników dających się porównywać z kampaniami wzorcowymi**

Zalety

- Skupiony zespół dbający o ciągłość programu
- Program indywidualnie dostosowany i skrojony pod kątem wymagań klienta
- Pomoc w zmniejszaniu zależności od istniejących umiejętności pracowników
- Oficjalny program uświadamiania i szkoleń w zakresie bezpieczeństwa
- Bieżące zarządzanie programem

Korzyści

- Pomoc w zmniejszeniu liczby incydentów w dziedzinie bezpieczeństwa
- Pomoc w minimalizacji ogólnego kosztu incydentów
- Spójność wdrożenia w skali całej organizacji
- Połączenie prowadzonych na żywo prób ataków phishingowych z ukierunkowanymi pod ich kątem szkoleniami
- Pomoc w zwiększaniu stopnia uświadomienia w dziedzinie bezpieczeństwa i wprowadzaniu zmian w zachowaniach