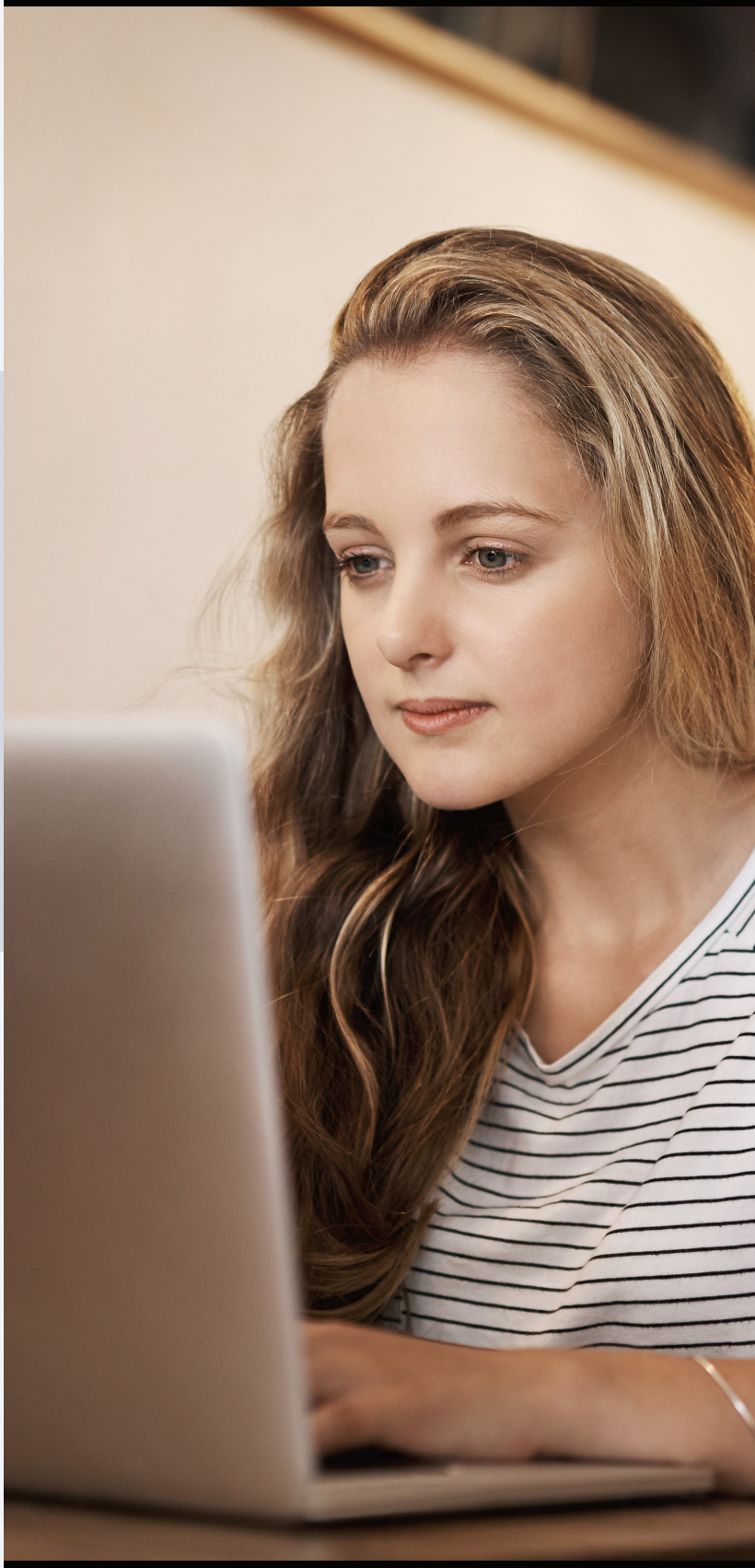
Stärkung der ersten Verteidigungslinie und des schwächsten Glieds: Menschen.

IBM Security



Die beste Möglichkeit für Mitarbeiter, ein Unternehmen vor Cyber-Sicherheitsbedrohungen zu schützen: sie dürfen niemals E-Mails öffnen.
Ein besserer Plan ist es, Mitarbeiter zu schulen.

IBM Security – Dienstleistungen für Sensibilisierung und Schulungen

IBM Security bietet eine umfassende Programmentwicklung sowie eine kontinuierliche Anpassung des Sicherheitsbewusstseins und Phishing-Schulungen – zur Förderung einer risikobewussten Kultur. Wir bieten ein maßgeschneidertes und kontinuierliches Sensibilisierungsprogramm für Ihre Organisation.

Phishing bleibt ein Top-Bedrohungsvektor, und unsere Dienste helfen Mitarbeitern dabei, besser gegen Phishing und Social Engineering gewappnet zu sein. Wir schulen Ihre Mitarbeiter in den Bereichen eLearning, Gamifizierung, Phishing und Social-Engineering-Simulationen. Unsere erfahrenen Berater bieten Plattformanpassung, maßgeschneiderte Schulungsmethoden, Metriken, Berichterstattung und Programmmanagement.

Legen Sie noch heute los!
Erfahren Sie mehr über die Vorteile eines Programms für Sicherheitsbewusstsein und Schulungen.

Kontaktieren Sie IBM Security Services unter:
ibm.biz/BdqYUF.

IBM

Ein umfassendes Programm für Sicherheitsbewusstsein und Schulungen kann dazu beitragen, das organisatorische Risiko zu mindern.

Fünf Schritte zur Programmentwicklung.

1. Definieren

- **Programmziele definieren**
- **Zielpublikum definieren (Umfang)**
- **KPIs definieren**
- **Programm- und Compliance-Anforderungen definieren**

2. Einrichten

- **Einen Cyber-Bewusstseinsrahmen einrichten**
- **Einen Sensibilisierungsplan aufstellen**
- **Artefakte und Schulungsleitfäden erstellen**
- **Unterstützung der Führungsebene gewinnen**

3. Bewerten

- **Den aktuellen Stand des Wissens über Informationssicherheit einschätzen**
- **Den aktuellen Stand des Verständnisses von Mitarbeitern für ihre Rolle und Fähigkeiten zur Informationssicherheit bewerten**

4. Implementieren

- **Integrationen und Anpassungen durchführen**
- **Schulungen, Kampagnen, Quizfragen und Umfragen durchführen**
- **Einrichtung von computerbasierten Schulungen für Teilnehmer/innen**

5. Messen

- **Die Effektivität des Programms verfolgen und messen**
- **Reports über Assessments und Schulungen erstellen**
- **Vergleichbare Ergebnisse mit Baseline-Kampagnen erzielen**

Nutzen

- Fokussiertes Team für ein kontinuierliches Programm
- Maßgeschneidert und auf Kundenbedürfnisse zugeschnitten
- Hilft, die Abhängigkeit von internen Kompetenzen zu verringern
- Formelles Programm für Sicherheitsbewusstsein und Schulungen
- Laufende Verwaltung des Programms

Vorteile

- Hilft, die Zahl der Zwischenfälle zu reduzieren
- Hilft, die Gesamtkosten von Zwischenfällen zu minimieren
- Konsistente Implementierung im gesamten Unternehmen
- Verknüpft Live-Phishing-Tests mit gezielter Schulung
- Hilft, das Sicherheitsbewusstsein zu verbessern und Verhaltensänderungen zu erzielen