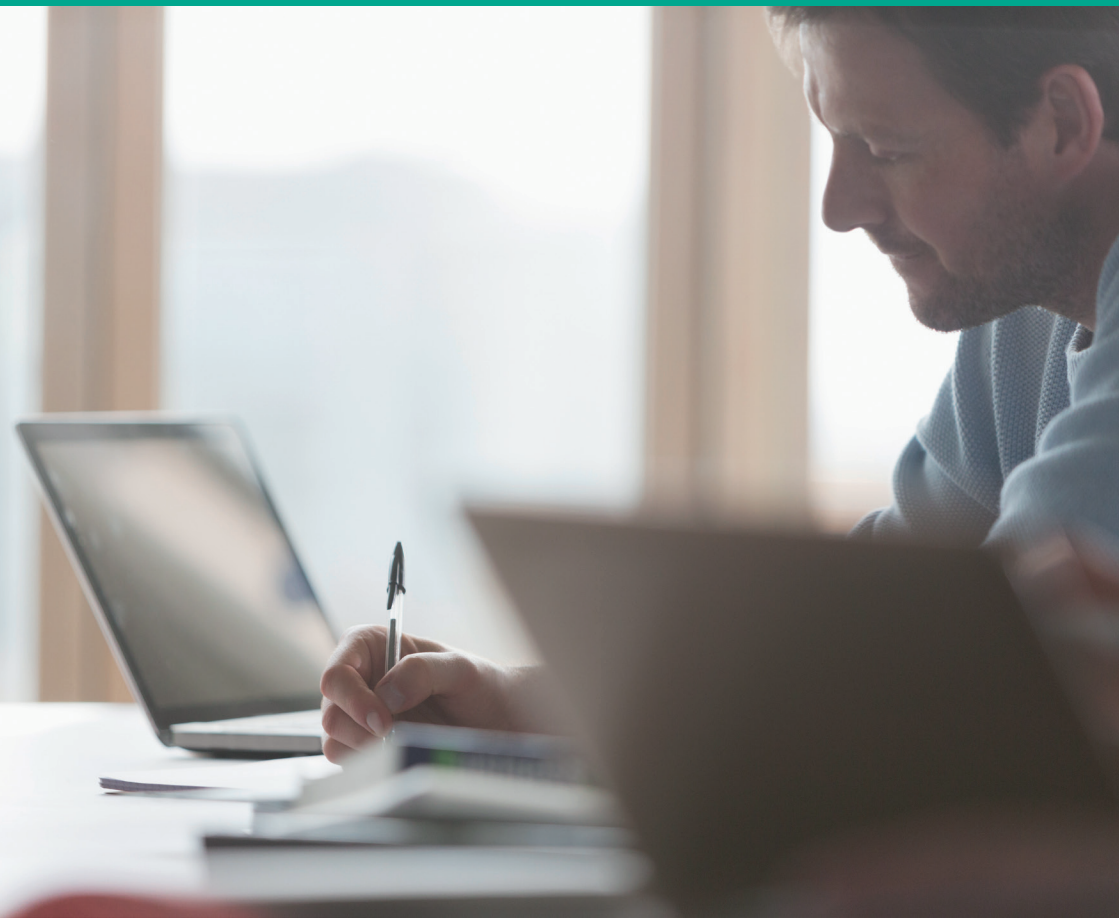


Kaspersky Security Education Platform

Interaktive Onlineschulungen
für Mitarbeiter aller Abteilungen

Kaspersky®
Cybersecurity
Awareness Training

Kaspersky Security Education Platform

Rund 80 Prozent der **Cybervorfälle** beginnen mit dem **Risikofaktor Mensch.** Umso wichtiger ist ein umfassendes Schulungsprogramm für alle Mitarbeiter. Kaspersky Security Education Platform hilft, potenzielle Gefahren besser zu erkennen und das **Bewusstsein für Cybersicherheit** zu steigern.

Mangelndes Wissen über gängige Angriffstechniken und Betrugsmethoden sind in der Regel der Grund, warum Mitarbeiter zum **Einfallstor für Cyberattacken** werden. So fallen sie beispielsweise Phishing-Mails zum Opfer. In täuschend echt aussehenden E-Mails werden Mitarbeiter dazu aufgefordert, Benutzernamen, Passwörter oder PINs preiszugeben.

Die modulare Onlineschulungsplattform von Kaspersky Lab richtet sich an **alle Mitarbeiter eines Unternehmens.** In interaktiven Übungen und anhand typischer Szenarien des Arbeitsalltags lernen die Teilnehmer direkt an ihrem Computer mehr über **potenzielle IT-Bedrohungen** sowie den Umgang damit.

Dabei sind die Online-Schulungen individuell auf die jeweiligen Mitarbeiter zugeschnitten. Je nach persönlichem Kenntnisstand im Bereich Cyberbedrohungen und der tatsächlichen Bedrohungslage, der ein Mitarbeiter bei seiner Arbeit ausgesetzt ist, lassen sich **unterschiedliche Schwierigkeitsstufen** auswählen.

Vorteile für die Mitarbeiter

- 25 Lernmodule mit 15-20 Minuten pro Modul (Stand: Juni 2017)
- Erweiterung technischer Fähigkeiten in der Cybersicherheit
- Sicherer Umgang mit sozialen Netzwerken, physischer Sicherheit, mobilen Geräten, gefährlichen Links im Internet, E-Mails sowie Passwörtern
- Mehr Wissen in verschiedenen Bereichen wie zum Beispiel Datenschutz, Sicherheit außerhalb des Arbeitsplatzes und Social Engineering
- Erkennen von Phishing-Angriffen und gefährlichen Links in E-Mails
- Entwicklung von Verständnis und Bewusstsein für die Wichtigkeit von Cybersicherheit
- Ermittlung des eigenen Wissens durch Wissenstests

Vorteile für das Unternehmen

- Ausbildung einer Cybersicherheitskultur bei allen Mitarbeitern im Unternehmen
- Stärkung der Kooperation mit der IT-Sicherheitsabteilung
- Ermittlung des Wissens der einzelnen Mitarbeiter
- Effektive, dauerhafte und messbare Sensibilisierung für Cybersicherheit
- Simulierte Phishing-Angriffe inklusive veränderbarer Vorlagen in verschiedenen Bereichen
- Analyse und Fortschrittsberichte (z. B. gruppenspezifisch, nach Standort, etc.)
- Durchführbar während der Arbeitszeit aufgrund der geringen aufzuwendenden Zeit von 15-20 Minuten pro Modul

Unsere Lernmodule (Stand: Juni 2017)

Anti-Phishing Phil
Lernen Sie, wie Sie Phishing-Angriffe erkennen, indem Sie betrügerische URLs entlarven.

Anti-Phishing Phyllis
Lernen Sie, wie Sie Phishing E-Mails erkennen, indem Sie auf die typischen Warnsignale achten.

Datenschutz und Datenzerstörung
Sichern Sie sich beim Einsatz von tragbaren Datenspeichern ab und entsorgen Sie sensible Daten ordnungsgemäß.

E-Mail Sicherheit
Lernen Sie, wie Sie Phishing E-Mails, gefährliche Anhänge und andere Betrügereien per E-Mail erkennen.

Geschützte Gesundheitsdaten (PHI)
Lernen Sie, warum Sie Protected Health Information (PHI – geschützte Gesundheitsinformationen) schützen sollten und wie sie dies erreichen können.

Grundlagen der Sicherheit
Erkennen Sie Sicherheitsprobleme, denen Sie bei Ihren geschäftlichen und privaten Aktivitäten häufig begegnen.

Grundlagen der Sicherheit Geschäftsleitung
Erkennen und vermeiden Sie Gefahren, denen leitende Manager bei der Arbeit und zu Hause ausgesetzt sind.

Passwortsicherheit
Lernen Sie, wie Sie sichere Passwörter erstellen und verwalten.

PCI DSS
Erkennen Sie die Warnhinweise und verbessern Sie die Sicherheit Ihrer Kreditkartendaten.

Physische Sicherheit
Lernen Sie, Menschen und Eigentum zu schützen.

PII
Schützen Sie vertrauliche Daten über Ihre eigene Person, Ihren Arbeitgeber und Ihre Kunden.

Schutz gegen Ransomware
Lernen Sie, wie man Ransomware-Angriffe erkennt und abwehrt.

Sichere soziale Netzwerke
Lernen Sie, wie Sie soziale Netzwerke sicher und verantwortungsvoll nutzen.

Sicheres Surfen im Internet
Bewegen Sie sich sicher im Internet, indem Sie riskante Verhaltensweisen und typische Fallen vermeiden.

Sicherheit mobiler Apps
Lernen Sie, die Sicherheit mobiler Apps zu beurteilen.

Sicherheit mobiler Geräte
Nutzen Sie wichtige physische und technische Sicherheitsvorkehrungen, um Ihre Geräte und Ihre Daten zu schützen.

Sicherheit über das Büro hinaus
Vermeiden Sie typische Sicherheitsfehler, wenn Sie zuhause oder unterwegs arbeiten.

Soziale Betrügereien
Erkennen und vermeiden Sie, dass sich Betrüger Ihre Daten durch soziale Manipulationen erschleichen.

URL-Schulung
Lernen Sie, wie man betrügerische URLs entlarvt.

USB-Gerätesicherheit
Schützen Sie beim Gebrauch von USB-Geräten Daten, Systeme und sich selbst.

Datenschutz-Grundverordnung
Erfahren Sie, wie sich der Schutz personenbezogener Daten unter der neuen Datenschutz-Grundverordnung (DSGVO) der Europäischen Union demnächst ändert.

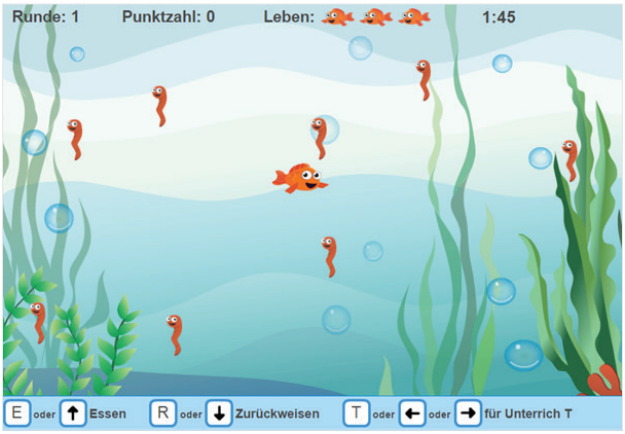
Einleitende Hinweise zum Phishing
Erkennen Sie E-Mail-Fallen und vermeiden Sie Phishing-Betrügereien.

Sicherheit auf Reisen
Lernen Sie, wie man Daten und Geräte beim Arbeiten in Flughäfen, in Hotels, auf Konferenzen und an anderen öffentlichen Orten sicher hält.

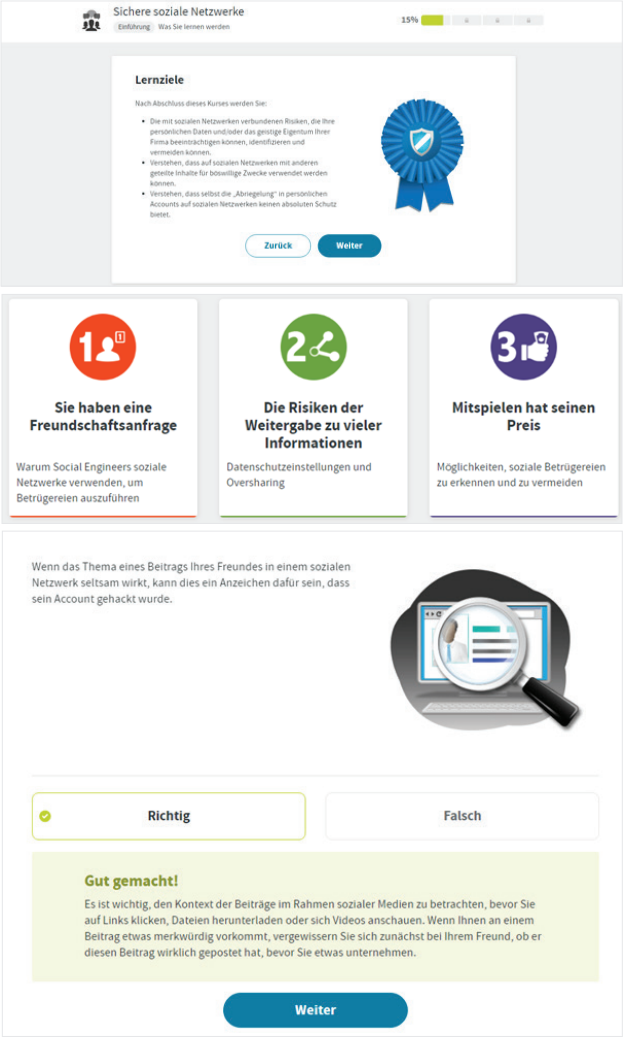
Vermeidung gefährlicher Anhänge
Identifizieren und vermeiden Sie gefährliche E-Mail-Anhänge.

Vermeidung gefährlicher Links
Erkennen Sie gängige E-Mail-Fallen und vermeiden Sie gefährliche Links.

Beispiele der Lernmodule



Beispiel aus dem Lernmodul „Anti-Phishing Phil" inklusive Auswertung



Beispiel aus dem Lernmodul „Sichere soziale Netzwerke“ inklusive einer Richtig-/Falsch-Frage

Umfassende Administrationsmöglichkeiten

Der Bereich **„ThreatSim Phishing“** ermöglicht Simulationen von Phishing-Attacken, um die Reaktionen der Mitarbeiter zu testen. Beispiele für Phishing-E-Mails werden mitgeliefert und können vom Administrator nach Belieben verändert werden. Sobald ein Mitarbeiter eine dieser E-Mails anklickt, öffnet sich ein Warnhinweis mit einigen grundlegenden Ratschlägen. Automatisch können dann beliebige Schulungsmodule zugewiesen werden. Ein umfangreiches Berichtswesen ist ebenso integriert, mit dem der Administrator eine Auswertung der unterschiedlichen Phishing-Kampagnen machen und diese auch miteinander vergleichen kann.

Im Bereich **„Assessments“** kann der Administrator den Mitarbeitern vorgefertigte oder selbst erstellte Wissenstests zur Verfügung stellen, um somit den Schulungsbedarf des einzelnen Mitarbeiters zu erkennen.

Mit einem Zugang pro Mitarbeiter können die 25 Online-Lernmodule (Stand: Juni 2017) individuell zugewiesen werden.

Diese können auf einzelne Nutzer und/oder Gruppen zeitlich aufgeteilt und mit einer Reminder-Funktion versehen werden. Zugleich gibt es die Möglichkeit, am Anfang und/oder am Ende eine individuell gestaltete Folie einzubauen, zum Beispiel als Begrüßung oder mit speziellen Richtlinien im Unternehmen.

Der Bereich **„Reports“** ermöglicht die Erstellung von unterschiedlichen und umfangreichen Berichten, um den Kenntnisstand der Mitarbeiter sowie ihre Fortschritte über einen bestimmten Zeitraum zu bewerten.

- ✓ Pro Mitarbeiter
- ✓ Pro Gruppe
- ✓ Pro Modul
- ✓ Auswertung Wissenstest, uvm.

Die Berichte können in eine Excel-, Word- und CSV-Datei exportiert werden.

Mithilfe der Auswertung kann der Administrator einen Schulungsplan zur Cybersicherheit aufstellen und so die Entwicklung der Mitarbeiter mittels einfacher bis schwieriger Lektionen in unterschiedlichen Bereichen der IT-Sicherheit fördern.

Notizen

t4iva/Stand: Juni 2017

Kaspersky Lab GmbH, Ingolstadt, Deutschland
www.kaspersky.de
Informationen zur Internetsicherheit: www.viruslist.de
Informationen zum Thema Awareness finden Sie hier:
https://www.kaspersky.de/enterprise-security/cybersecurity-awareness

www.kaspersky.de