teleinformatik

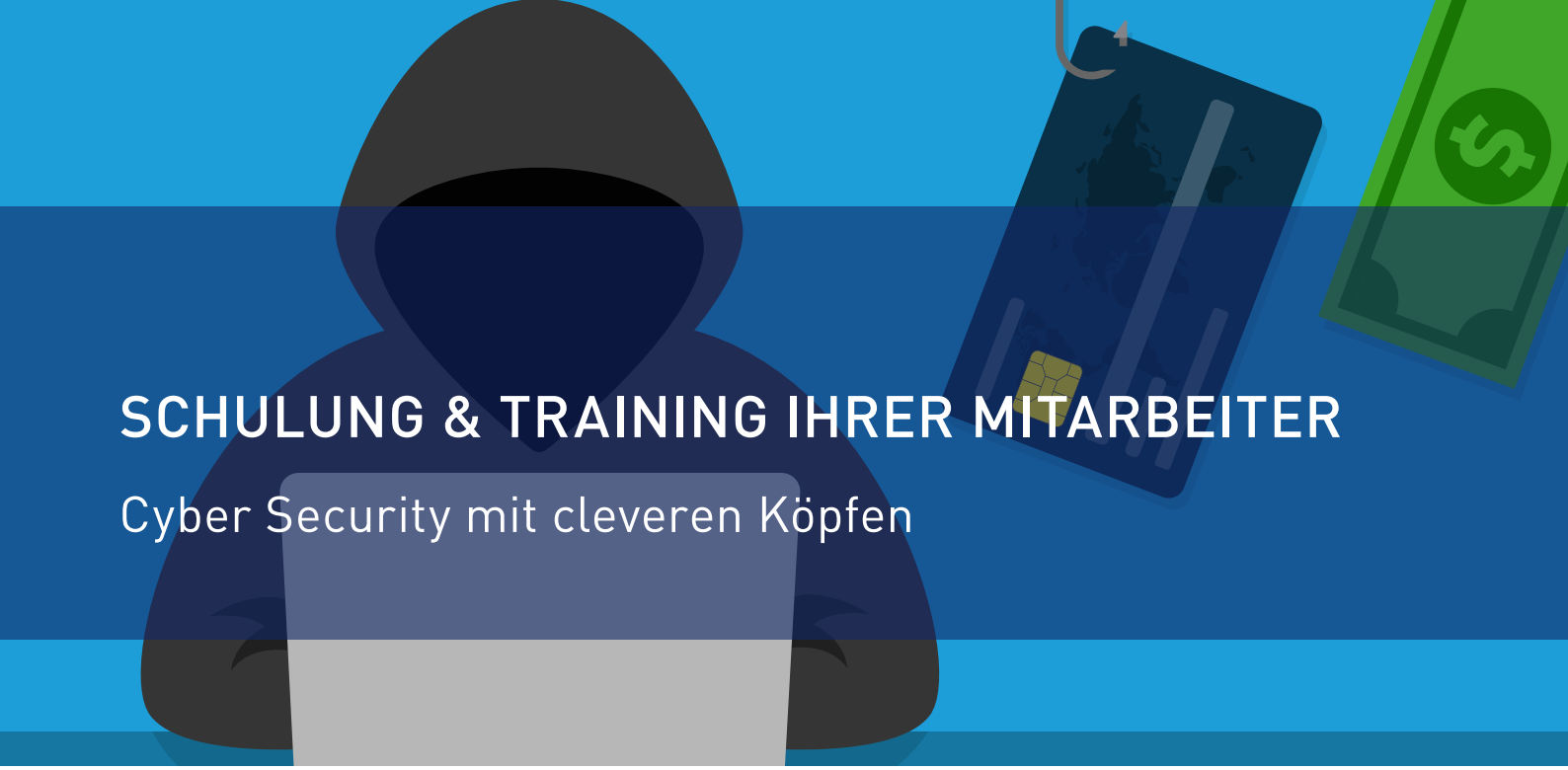
IT & Communications Solutions since 1999

MIND SECURITY

F

SCHULUNG & TRAINING GEGEN PHISHING ATTACKEN

Für bewussten Umgang mit Cyber Security



SCHULUNG & TRAINING IHRER MITARBEITER

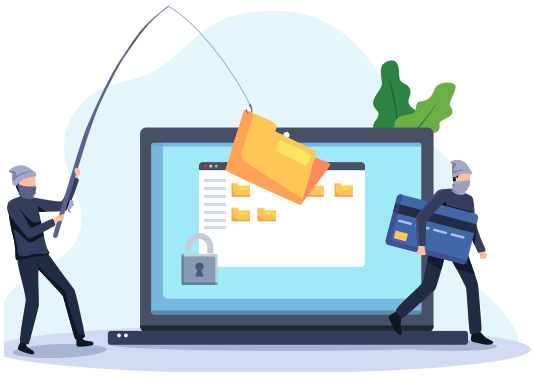
Cyber Security mit cleveren Köpfen

SICHERHEITSLÜCKE NR. 1 - FAKTOR MENSCH

Jede IT-Infrastruktur ist angreifbar, wenn der Faktor **«Mensch»** als E-Mail Empfänger nicht ebenso sensibilisiert ist, denn 9 von 10 Cyberattacken beginnen beim User. Mit unserer neuen und effizienten Massnahme **MIND SECURITY** ermöglichen wir Ihnen, in Ihrem Unternehmen eine Sicherheitskultur aufzubauen und Risiken mit Sensibilisierungsprogrammen zu mindern.

Basierend auf Verhaltensforschung und intelligenten Algorithmen werden Angriffssimulationen vorgenommen, mit denen Ihre Mitarbeiter vorgetäuschte Phishing-E-Mails erhalten. Diese werden absichtlich sowie gut getarnt verschickt und enthalten Links oder Anhänge, die ungefährlich sind und lediglich auf eine interaktive e-Learning Plattform führen.

ABLAUF MIND SECURITY TRAINING



1. INITIALPHASE: PHISHING E-MAIL SIMULATION

Während den ersten 2 Wochen werden 3 als Phishing gut getarnte E-Mails mit Links und Anhängen an die Mitarbeiter verschickt.

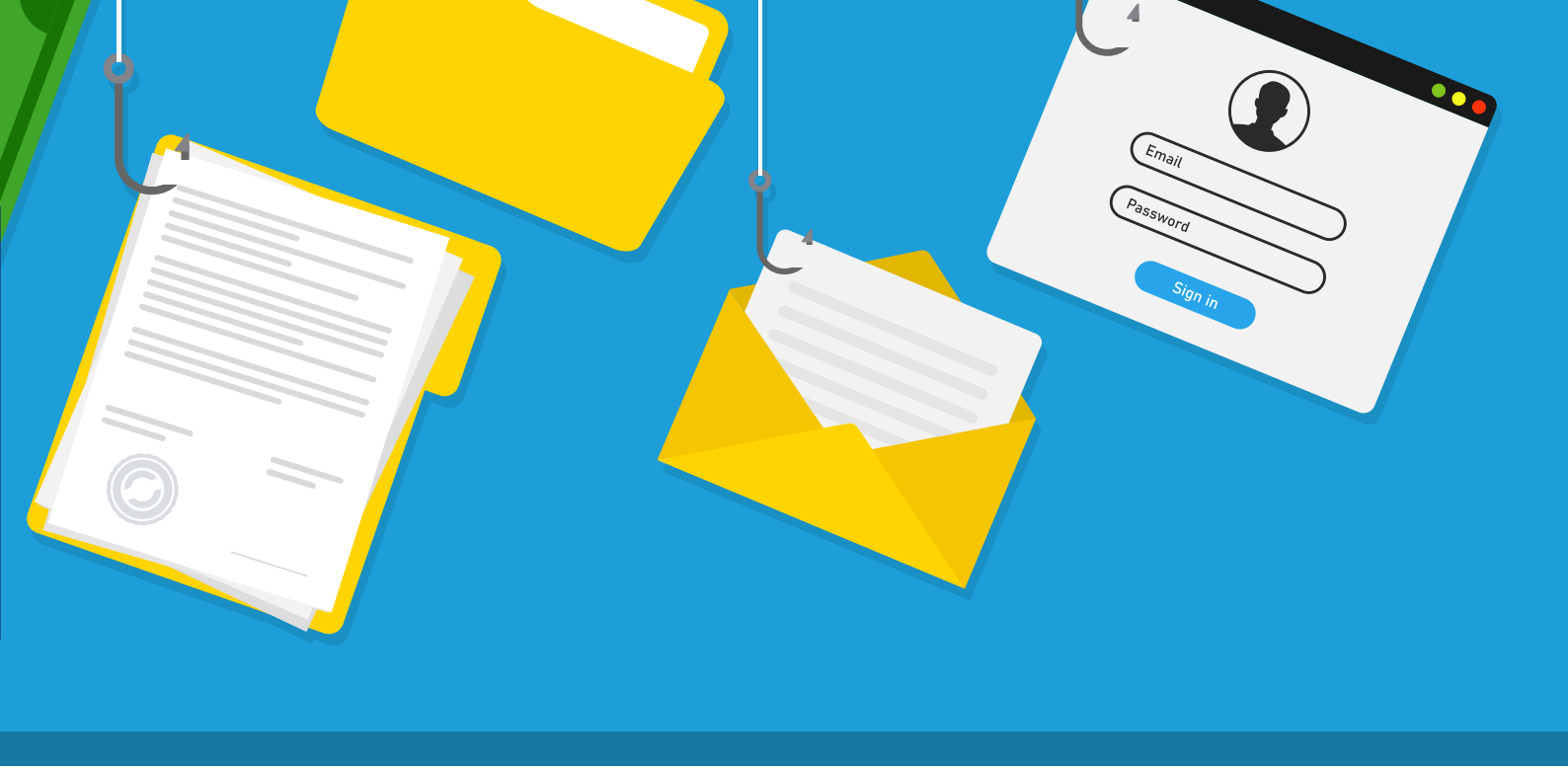
Monitoring & Reporting System

Nach der Auswertung der ersten 2 Wochen und Präsentation der Ergebnisse wird das E-Learning-Management-Systems für die Mitarbeiter freigeschaltet.

2. FOLGEPHASE - E-LEARNING

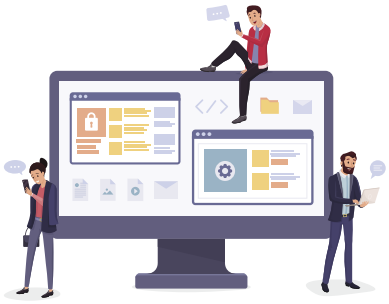
Auf das restliche Jahr verteilt werden 9 weitere als Phishing-E-Mails getarnte Nachrichten an die Mitarbeiter verschickt.

Ihre Mitarbeiter können an Schulungsmodulen teilnehmen und Wissenswertes über Cyber Security und dessen Risiken lernen.



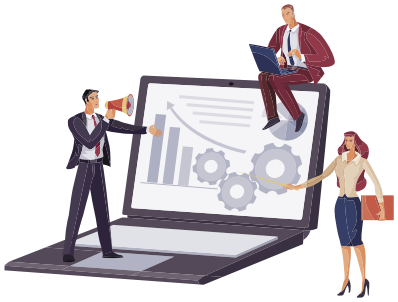
STEIGERUNG DER ABWEHRFÄHIGKEIT

Die **MIND SECURITY-e-Learning-Plattform** schult Ihre Mitarbeiter auf vielfältige Art und Weise und ermöglicht Ihnen so, das Risikobewusstsein Ihrer Mitarbeiter entscheidend zu schärfen. Dadurch versetzen Sie Ihr Unternehmen in die Situation, Risiken frühzeitig zu erkennen und Schäden erfolgreich abzuwenden.



UMFASSENDE ANALYSEN

Mit dem Tracking- & Reporting System werden die Reaktionen laufend gemessen und melden Ihnen anonym, wo allfällige Schwachstellen liegen. Ziel ist es, Transparenz über die aktuelle Anfälligkeit für Phishing-Angriffe zu erlangen.



VORTEILE

Ihre Mitarbeiter werden auf Hackerangriffe regelmässig sensibilisiert und gehen bewusster um mit verdächtigen E-Mails.

STEIGERUNG RISIKOBEWUSSTSEIN

Klicken Nutzerinnen oder Nutzer auf eine simulierte Phishing-Mail, gelangen sie zu einer Lernseite mit individuellen Hinweisen zu Cyber Security, vollkommen anonym.

TRANSPARENZ ANFÄLLIGKEIT

In einem Analytics-Dashboard können alle wichtigen Klick- oder Login-Raten jederzeit eingesehen werden, wie auch die erfolgreichsten psychologischen Taktiken identifizieren.

E-LEARNING PLATTFORM

Das E-Learning umfasst praxisnahe und interaktive Module zu IT-Sicherheits- und Datenschutzthemen. Jedes Modul beinhaltet konkrete Handlungsempfehlungen.

VERSCHIEDENE ANGRIFFSATTACKEN

Cyber-Angriffe im privaten wie im beruflichen Kontext nehmen stetig zu und gestalten sich unter anderem je nach Unachtsamkeit der Mitarbeiter für die Cyberkriminellen relativ einfach.

PHISHING

«Abfischen» von Passwörtern über präparierte E-Mails, Nachrichten oder Anrufe.

z. B. Abfrage des Passwortes über eine gefälschte Anmeldemaske.

BRUTE FORCE

Automatisierter Angriff auf die Anmeldemaske selbst, bei der schwache Passwörter mit «roher Gewalt» gehackt werden.

z. B. systematisches Durchtesten von Wörter- und Zeichenkombinationen mit Hilfe passender Wortlisten.

MALWARE

Schadprogramme, die sich unbemerkt auf dem Computer des Opfers im Hintergrund installieren.

z. B. Protokollierung der Tastatureingaben durch sogenannte «Key Logger».

SOCIAL ENGINEERING

Gezielte Informationsbeschaffung über die Zielperson oder das Unternehmen, um ein naheliegendes Passwort zu erraten.

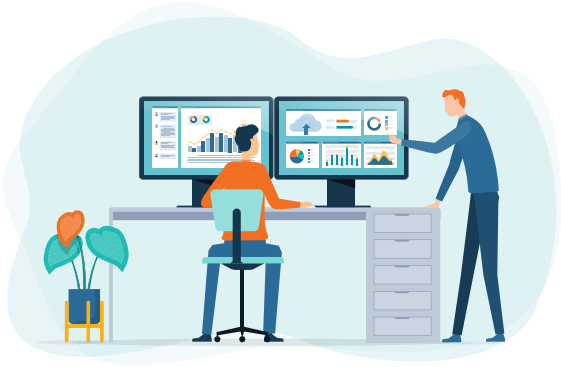
z. B. schauen sich Cyberkriminelle Ihr Profil in den sozialen Medien an, sehen, dass Ihr Hund «Rex» heisst und probieren dies dann als Passwort aus.

UNSERE PAKETE

Pakete	3 E-Mails während 2 Wochen	Monitoring & Reporting Dashboard	9 E-Mails während 50 Wochen	E-Learning-Management-System, 12 Module	Jahresauswertung	Lizenzkosten CHF **
Testpaket für 2 Wochen unlimitierte Benutzeranzahl	✓	✓	-	-	-	450.- einmalig
Vollversion 12 Monate* ab 11 Benutzer	✓	✓	✓	✓	✓	3.90 pro Benutzer monatlich
Vollversion 12 Monate* bis 10 Benutzer	✓	✓	✓	✓	✓	4.90 pro Benutzer monatlich

UNVERBINDLICHE TESTPHASE

Mit dem Testpaket haben Sie die Möglichkeit, mit den Simulationen der Phishing E-Mails zu prüfen, wie viele davon effektiv von den Benutzern angeklickt werden. Anhand des Trackings und Reportings können wir gemeinsam die weiteren Schritte oder Massnahmen planen sowie mit den Schulungen anschliessend gleich für 12 Monate starten.



* Verlängerung ist jederzeit möglich.

** Die Preise sind exkl. Einrichtungskosten

HABEN WIR IHR INTERESSE GEWECKT?

Telefon +41 44 315 15 15

TELEINFORMATIK SERVICES AG
SCHULSTRASSE 37, 8050 ZÜRICH
WWW.TELEINFORMATIK.CH