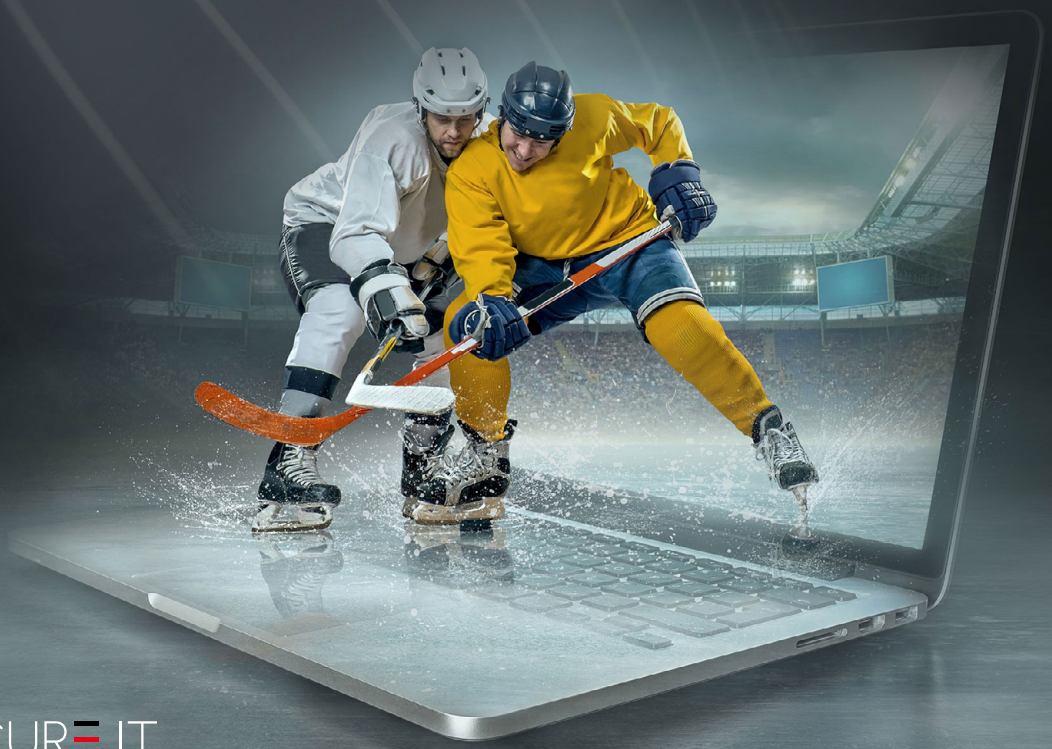
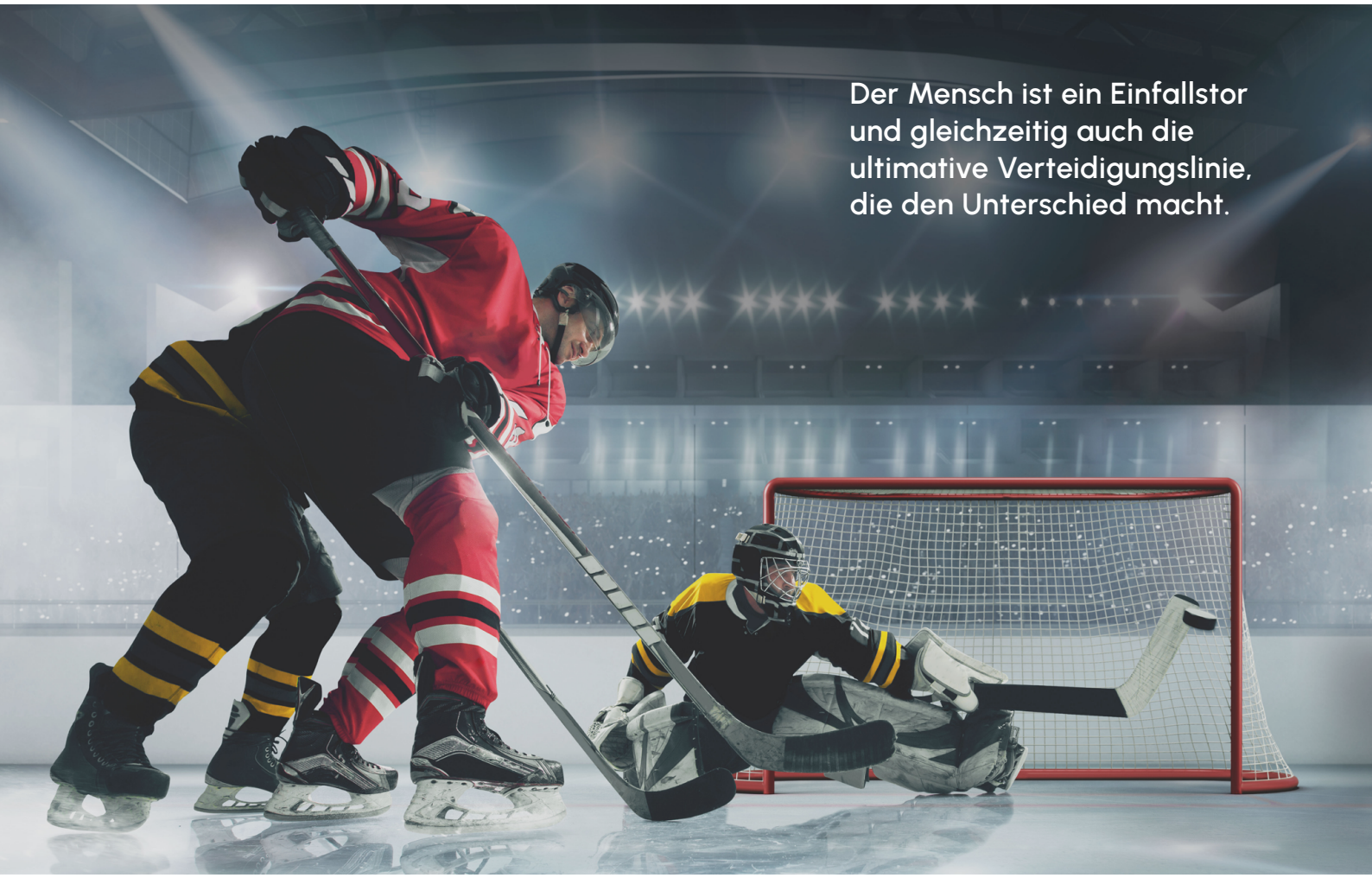
DriveLock

SECURITY AWARENESS

Stärken Sie Ihre menschliche Firewall



HYPERSECURE IT

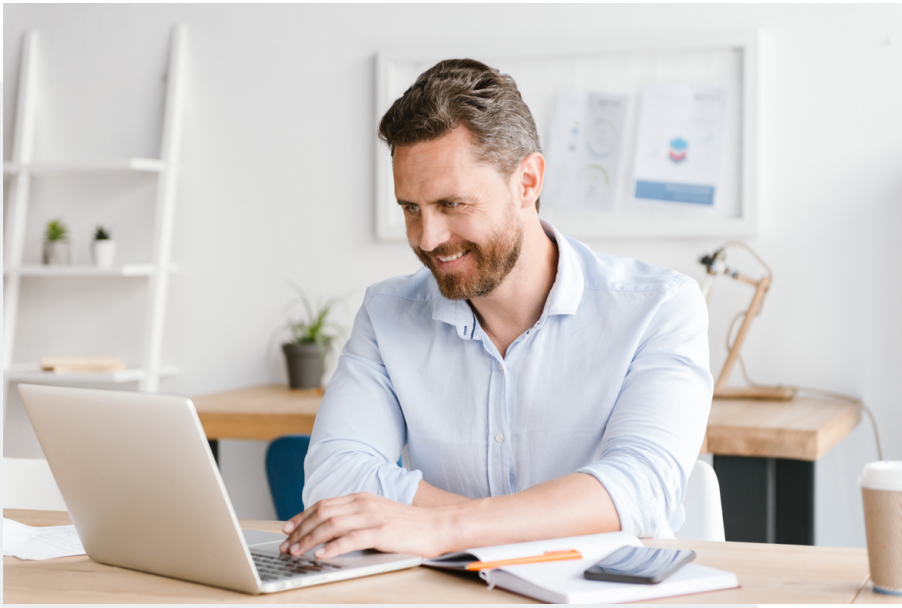


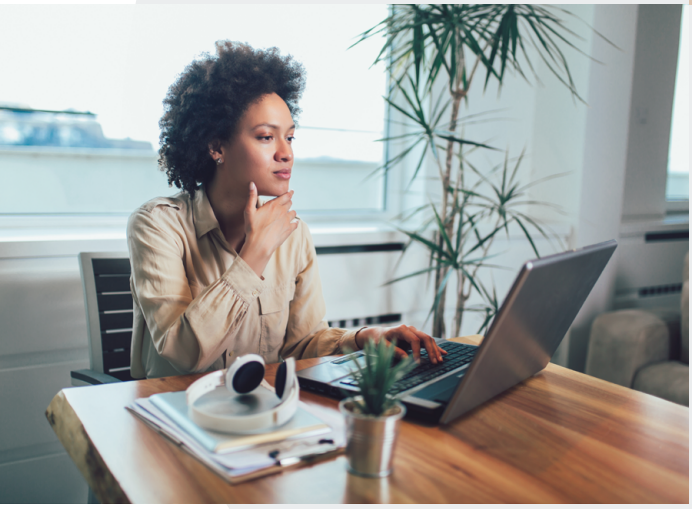
Cyberabwehr und Prävention

Es geht darum, Systeme und Menschen zu schützen

Wenn wir über Cybersecurity sprechen, denken wir zunächst an technisch ausgefeilte Sicherheitsmaßnahmen. Die wichtigste Sicherheitsmaßnahme ist aber der Mensch. Es wäre zu einfach, Cyberabwehr als rein technische Herausforderung zu betrachten, die mit Präventionsmaßnahmen wie Antivirenscanner, Firewall oder Applikationskontrolle zu stemmen ist: Letztlich geht es immer darum, sowohl Systeme als auch Menschen zu schützen, nicht Opfer von Angriffen zu werden. Das Handeln von Menschen spielt dabei eine entscheidende Rolle. Ob eine Cyberattacke zum Erfolg führt oder nicht, verantworten Menschen. Meist sind Angriffe die Folge eines bewussten oder unbewussten Insiderjobs. Wenn man den Menschen als wichtigstes Glied einer ganzheitlichen Sicherheitsstrategie betrachtet, dann gehört die Sensibilisierung der Mitarbeiter genauso zum Maßnahmenspektrum wie die bereits genannten technischen Abwehrmaßnahmen, zu denen auch die präventive Vereitelung eines potenziellen Datendiebstahls durch Verschlüsselung von Daten, Dateien und Festplatten zählt. Es gilt, die Belegschaft für das Thema IT-Sicherheit zu aktivieren und sensibilisieren und Ihnen zu erklären, wie wichtig sie selbst innerhalb der Kette von Schutzmaßnahmen sind. Hier ist ein Zusammenspiel zwischen IT-Abteilungen, Mitarbeitern und Personalabteilung gefragt. Ein Unternehmen kann nur dann eine erfolgreiche Sicherheitsstrategie aufbauen, wenn alle Beteiligten motiviert sind, die Maßnahmen umzusetzen und wenn sie den Schutz vor Angriffen und Datenmissbrauch verinnerlicht haben.

Homeoffice



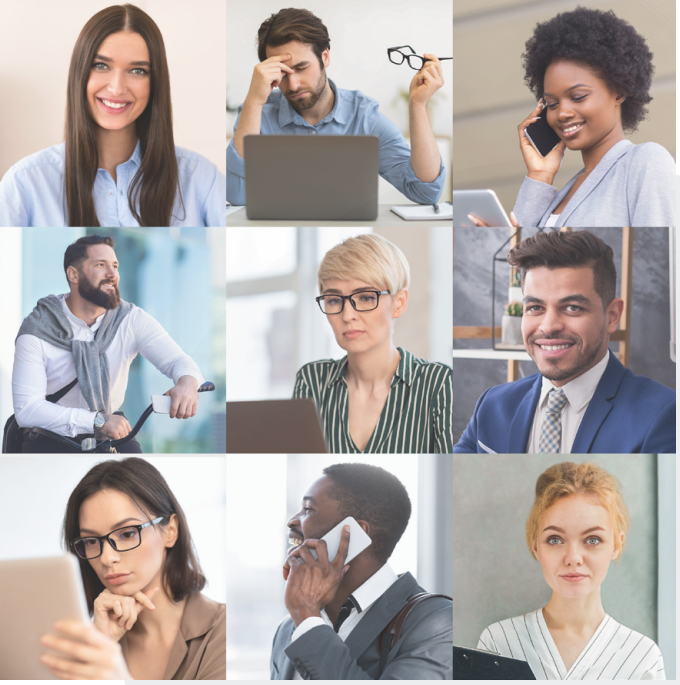


Trend zu Remote Arbeit verschärft die Sicherheitslage

Bei der Heim- oder Remote Arbeit sind Menschen besonders gefordert. Mitarbeiter, die von zu Hause aus arbeiten, sind aufgrund teils mangelhafter technischer Kontrollen und oftmals zu sorglosem Sicherheitsbewusstsein in der Gefahr, Dinge zu tun, die negative Folgen für die Cybersicherheit in Ihrem Unternehmen haben könnten.

Sie können bei ihrer Arbeit von Familienmitgliedern oder Besuchern unterbrochen oder abgelenkt werden. Diese Ablenkungen können den Einzelnen unvorsichtig machen. Beispielsweise ist eine oft unterschätzte Gefahr die Verwendung von USB-Geräten. Die häufigsten Quellen für Viren- oder Malware-Infektionen sind USB-Geräte, da diese unwissentlich befallen sein könnten. Es fehlt der unmittelbare physische Kontakt zu Kollegen und der IT-Abteilung, bei der man sich auf dem kurzen Dienstweg Rat suchen kann.

Gerade in Zeiten hybrider Arbeit im Büro und zuhause wird Security Awareness immer wichtiger.



Mitarbeiter sensibilisieren durch Security Awareness Trainings

In Unternehmen sind IT-Sensibilisierungstrainings für alle Mitarbeiter – auch Vorgesetzte – mittlerweile unerlässlich, um Sicherheitsbewusstsein aufzubauen. Wichtig ist, dass diese Schulungen keine alleinstehenden, einmaligen Sondermaßnahmen sind.

Regelmäßiges Security Awareness Training mit kontextbezogenen Sensibilisierungsmaßnahmen schafft ein Bewusstsein, mit dem ein nachhaltiges Sicherheitsdenken etabliert werden kann. Dieses Training sollte alle Mitarbeiter erreichen, auch die Mitarbeiter, die technisch nicht versiert sind. Die Emotionen dieser Mitarbeiter sollten im Security Awareness Training angesprochen werden. Das Training soll Mut machen und motivieren, damit es wirken kann.

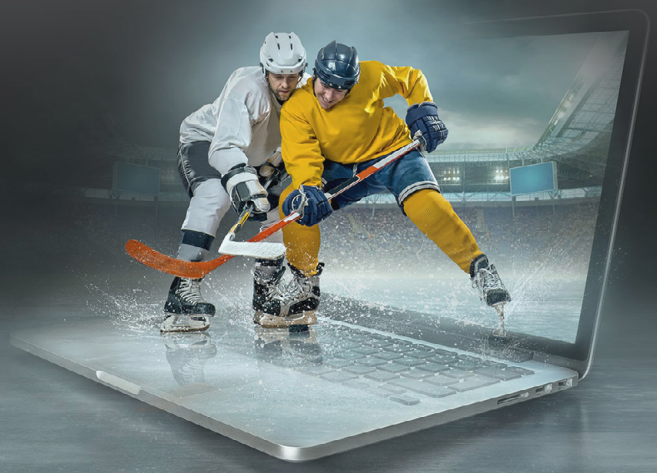
Ziele des Security Awareness Trainings

- Steigerung des Sicherheitsbewusstseins
- Dauerhafte Veränderung des Nutzerverhaltens
- Erfüllung von Empfehlungen und gesetzlichen Anforderungen, wie ISO 27001 oder BSI Grundschutz

Die wichtigsten Lerninhalte

Der Mensch als Firewall

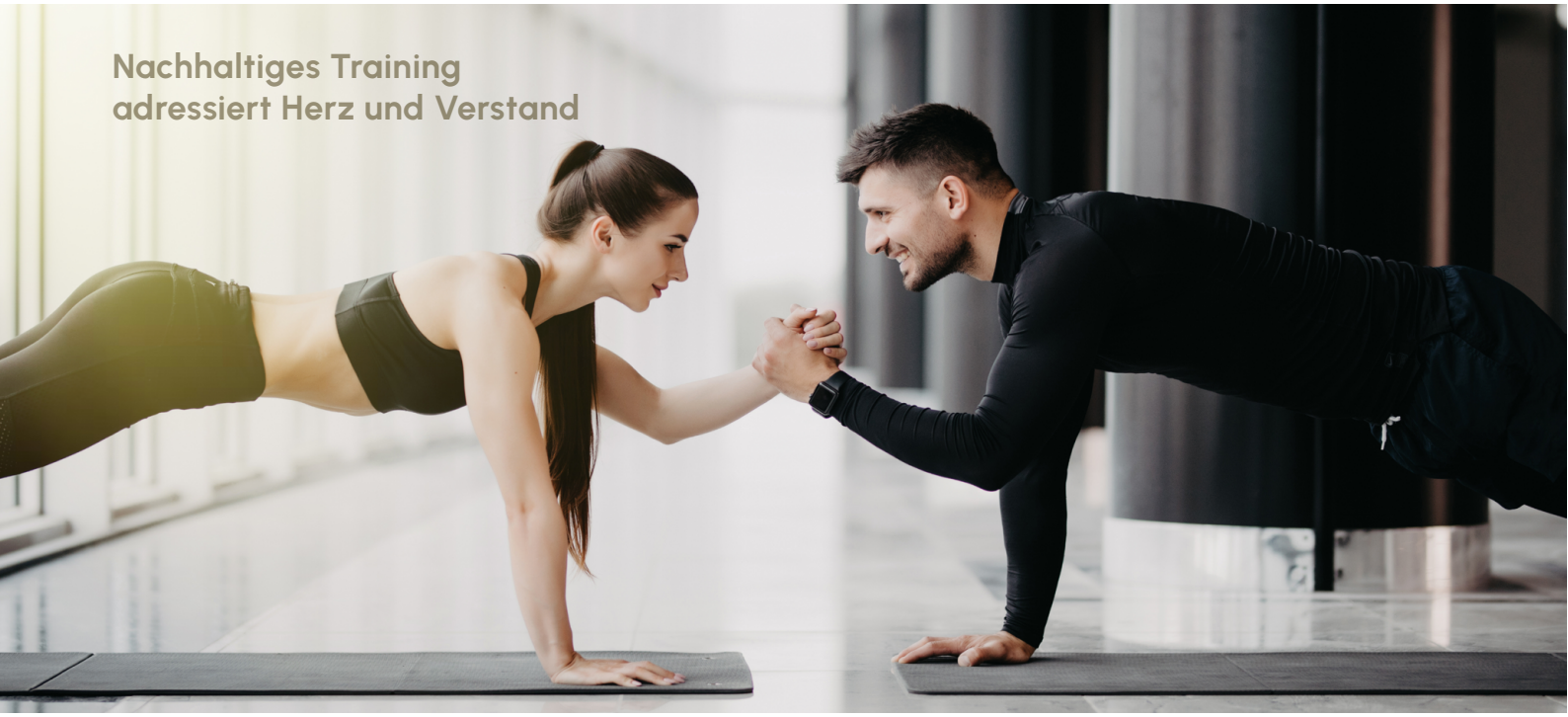
1. Social Engineering
2. Phishing E-Mails
3. Arbeiten in der Cloud
4. Sicherer Umgang mit USB-Geräten
5. Sicherer Umgang mit Benutzerkonten, E-Mails und Passwörtern
6. Außerhalb des Büros sicher arbeiten
7. Achtsamkeit im Umgang mit sensiblen Informationen
8. Datenschutzkonformer Umgang mit Informationen (EU-DSGVO)
9. Sichere Verwendung mobiler Geräte im Unternehmen (BYOD)



Security Awareness Training – Nachhaltigkeit

Wie erreichen Sie Nachhaltigkeit?

Viele Awareness-Programme scheitern aber in der Praxis, da IT-Security Awareness Methoden oftmals kaum die Wirkungszusammenhänge und Angriffsketten erklären, und die Programme nicht dauerhaft angelegt sind. Es werden zu viele (technische) Themen binnen kürzester Zeit geschult. Die Folge sind passive Teilnahme und geringer Spaßanteil. Regelmäßige, zielgruppengerechte Trainings, die mit Humor und Spaß das Wissen vermitteln sind am effektivsten. Nachhaltige Security Awareness Programme adressieren Herz und Verstand.



Tipps für nachhaltige Security Awareness Programme

TIPP 1
Stellen Sie sicher, dass die Beteiligten sich nicht nur der Bedeutung von IT-Sicherheit bewusst sind, sondern auch verstehen, warum sie wichtig ist. Ohne eine Verbindung zu schaffen, wird keine noch so gute Schulung das Verhalten langfristig ändern.

TIPP 2
Integrieren Sie ernste Themen, z.B. während eines Workshops, auch spielerisch und mit Humor.

TIPP 3
Setzen Sie moderne Lernmethoden ein, z.B. kurze Micro-Learnings und motivieren Sie Benutzer mit prägnanten Inhalten.

TIPP 4
Nutzen Sie experimentelles Lernen und spielerische Elemente (Gamification), um Verständnis zu schaffen, z.B. anhand einer simulierten Phishing E-Mail.

TIPP 5
Machen Sie sich Gedanken, wen Sie schulen: Jeder Mensch hat eine andere Auffassung von Sicherheit und daher ein anderes Gefühl für Relevanz.

TIPP 6
Der Mensch lernt durch Wiederholung. Unsere Vergessenskurve zeigt uns, wie das Erinnerungsvermögen mit der Zeit abnimmt. Deshalb sind Wiederholungen der einfachen Slogans wichtig.

TIPP 7
Schaffen Sie einen angstfreien Raum, anstatt Mitarbeiter öffentlich an den Pranger zu stellen, weil sie den falschen Link während ihrer Phishing-Trainings-Simulation angeklickt haben.

Security Awareness mit DriveLock

Integration in die HYPERSECURE Platform

DriveLock hat seinen Security Awareness Content in seiner IT-Security-Lösung verankert, der HYPERSECURE Platform.

Hinweise während des Arbeitens

Die Mitarbeitenden erhalten bei bestimmten Aktivitäten gezielte Hinweise, wie sie sich korrekt in Bezug auf Sicherheit verhalten sollen, z. B. beim Anschließen eines USB-Sticks. Dieser praktische Bezug ist wichtig, und führt oft zu einem „Aha-Erlebnis".

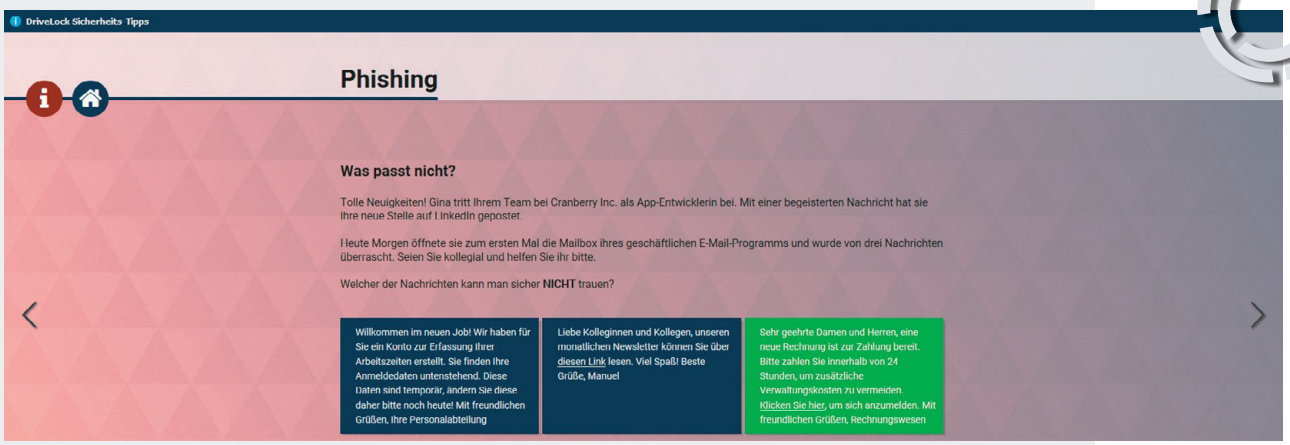
Hinweise beim Starten einer Applikation

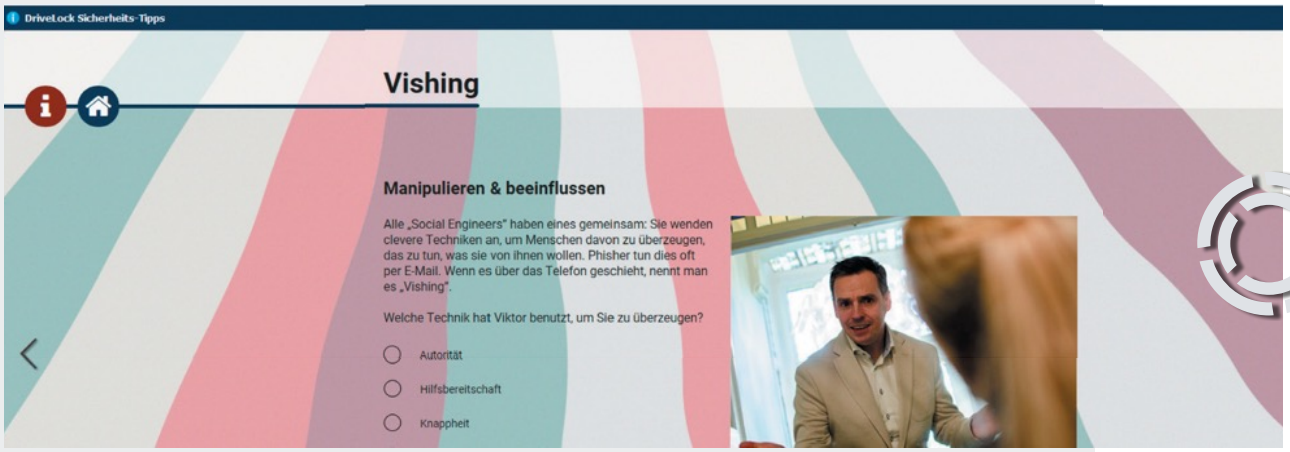
Beim Starten einer Applikation kann DriveLock überprüfen, ob es sich um eine sichere Anwendung handelt und eine kurze Kampagne mit Sicherheitshinweisen zum „Umgang mit neuen Anwendungen" abspielen.

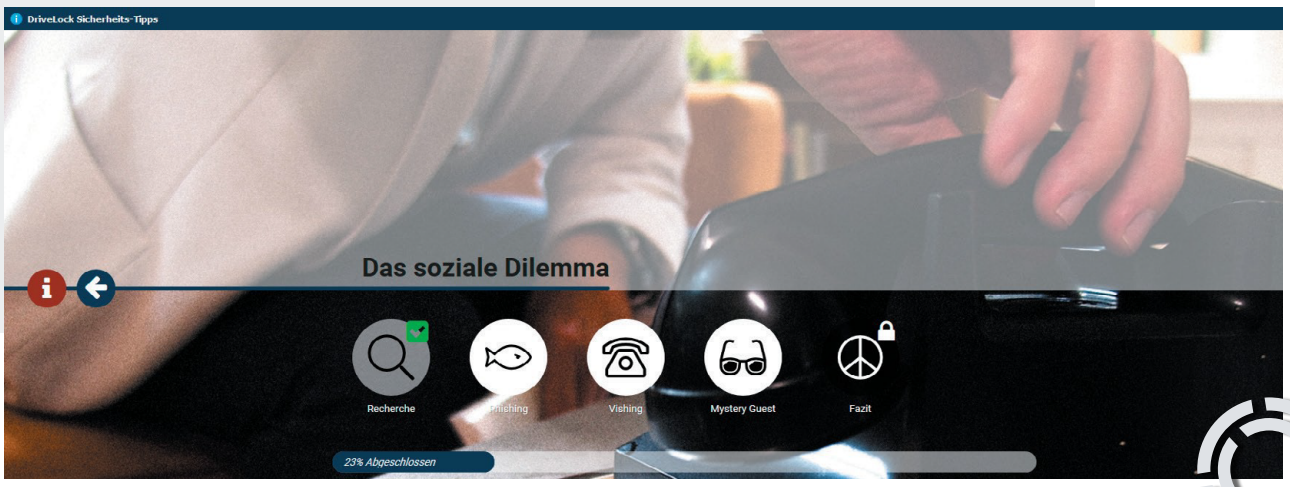
Lernen mit Spaß und Gaming-Faktor

Mit Multiple-Choice-Tests und Mikro-Lerneinheiten von wenigen Minuten mit Gaming-Faktor können Sie den Lernerfolg sofort eigenständig überprüfen und bei Bedarf vertiefen.

Security Awareness mit DriveLock







Starten Sie jetzt!

Security Awareness Training

Was können Sie sofort tun?

Praktische Tipps in Zeiten kritischer Cyberbedrohungslage

TIPP 1
Misstrauen Sie allen E-Mails, die Sie zu dringenden Handlungen auffordern. Geben Sie niemals Ihre Passwörter an und klicken Sie niemals auf Links oder Anhänge verdächtiger E-Mails. Dies gilt auch für E-Mails von Familie, Freunden oder dem Arbeitgeber, die unter Angabe eines gefälschten Absenders verschickt wurden.

TIPP 2
Überprüfen Sie bei allen Aktionen immer zuerst die Absender-E-Mail-Adresse, da der angezeigte Absendername sehr leicht gefälscht werden kann.

TIPP 3
Etablieren Sie im Unternehmen Meldeprozesse für Auffälligkeiten und Sicherheitsvorfälle. Richten Sie eine Unternehmensadresse ein, an die verdächtige Mails geleitet werden können. Dort sollten Sie Phishing E-Mails sammeln. Stellen Sie z. B. eine Intranet oder WIKI-Seite mit diesen Mails zusammen.

TIPP 4
Machen Sie die aktuelle Bedrohungslage (Warnhinweise vom BSI, Verfassungsschutz, etc.) Mitarbeiterinnen und Mitarbeitern bekannt, um ein Gefährdungsbewusstsein zu schaffen.

TIPP 5
Legen Sie Wert auf sichere, komplexe und regelmäßig zu ändernde Passwörter.
Um vertrauliche Daten zu schützen, sollten alle Angestellten sichere und komplexe Passwörter für ihre Geräte verwenden. Auch Datenträger sollten Sie mit Passwörtern schützen (Festplatte, Dateien, Wechseldatenträger).

TIPP 6
Wagen Sie den Schritt zur mehrstufigen Authentifizierung. Dieser sichere Schutzmechanismus macht es Angreifern schwer, in unternehmensinterne Systeme einzudringen und an sensible Daten zu kommen. Wo kein Passwort allein ausreicht, haben es Cyberkriminelle schwerer. Ziehen Sie auch andere Faktoren für das Identity & Access Management (IAM) in Betracht (Tokens, Biometrie).

TIPP 7
Gewähren Sie individuell oder gruppenbasiert Zugriffsrechte: Wenden Sie das Prinzip des „Least Privilege Access" (Prinzip der minimalen Privilegien) an. Benutzer sollen nicht mehr Zugriff haben als sie unbedingt benötigen.

TIPP 8
Animieren Sie Ihre Mitarbeiter, regelmäßig den Updatestatus ihrer Geräte und Software zu prüfen sowie ggf. Updates durchzuführen.

Kontaktieren Sie uns!

Testversion Security Awareness

DriveLock Security Awareness 30 Tage lang kostenlos und unverbindlich testen

Jetzt starten

Expertengespräch Security Awareness

Sprechen Sie kostenlos und unverbindlich mit einem unserer Experten über DriveLock Security Awareness

Termin vereinbaren

Mehr Information über DriveLock Security Awareness

Erfahren Sie mehr Interessantes und Wissenswertes über DriveLock Security Awareness auf unserer Webpage

Jetzt lesen

Wir unterstützen Sie gerne!

DriveLock SE
Landsberger Str. 396
81241 München

Tel. +49 (89) 546 36 49-0
E-Mail info@drivelock.com

DRIVELOCK.COM

HYPERSECURE IT

Mit der HYPERSECURE Platform
bleiben **Angriffe** auf IT-Systeme da,
wo sie hingehören: **außen vor**.