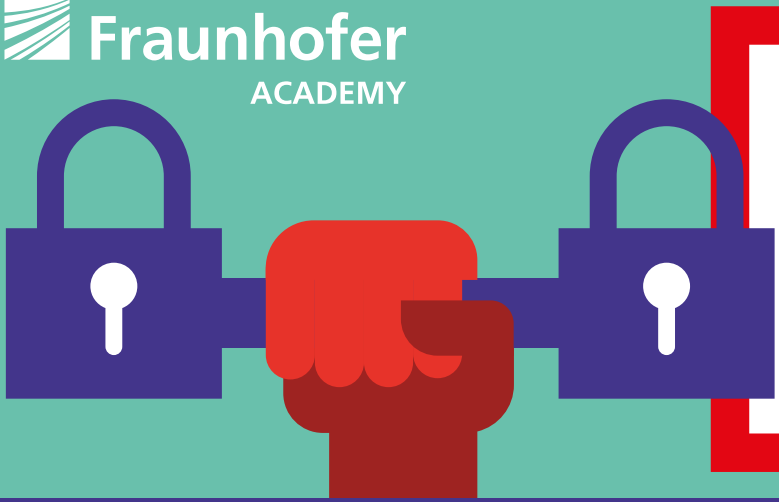
Fraunhofer
ACADEMY



IT-SECURITY-FITNESS-KALENDER

FÜR DEN BÜROALLTAG

Fraunhofer
ACADEMY

Es ist eine Binsenweisheit, die doch nicht häufig genug ausgesprochen werden kann: Wer regelmäßig Sport treibt, hat weniger Beschwerden im Alltag. Sie haben das bestimmt längst verinnerlicht und verhalten sich entsprechend vorbildlich. Deshalb zielt dieser Kalender auf Vorbeugung gegen Gefahren ganz anderer Natur: Er soll Ihre Sinne für die Tücken des Informationszeitalters schärfen und mit gänzlich neuen Übungen vor unnötigem Stress und übermäßiger Belastung schützen – kurzum: Ihre IT-Fitness stärken.

Wir wünschen viel Spaß mit unseren Anregungen – jeder Monat stellt eine innovative Sportart vor, deren Ausübung ein deutliches Plus an IT-Sicherheit für Ihren digitalen Alltag bietet.

Lernlabor
Cybersicherheit

Weiterführende Informationen zu diesen 12 IT-Security-Themen fi nden Sie unter: www.cybersicherheit.fraunhofer.de/it-security-fitness

Fraunhofer
ACADEMY

1 BACK-UP-YOGA

Back-up-Routinen etablieren

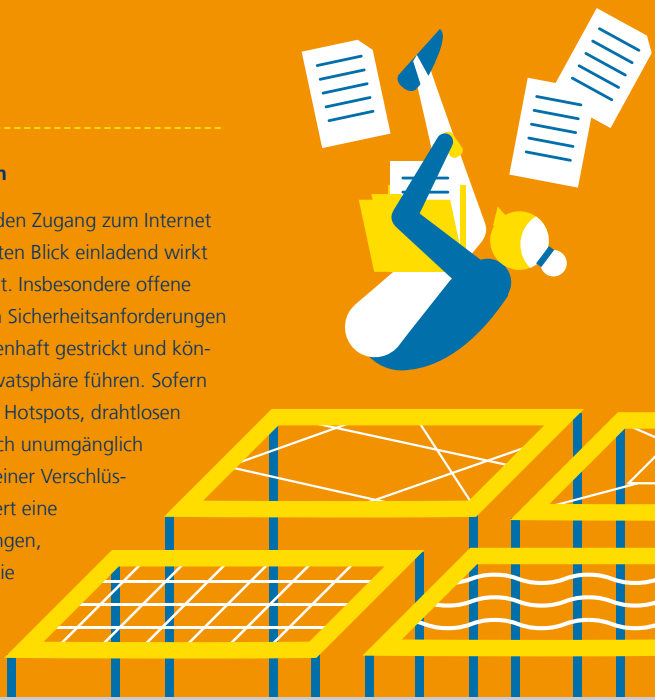
Schon wenige Minuten regelmäßiges Back-up-Yoga schenken einen deutlichen Zugewinn an Ausgeglichenheit und Souveränität. Kern der Philosophie dieses relativ neuen Yoga-Stils ist die Transzendenz wichtiger Informationen durch physische Spiegelung an einen sicheren Ort. Die einfach zu erlernenden Übungen werden routiniert und nahtlos in den Büroalltag integriert und bringen den Backup-Yogi auch bei unvorhergesehenen Ereignissen sofort wieder in Datenbalance.

Fraunhofer ACADEMY

2 WLAN-SPRINGEN

Auf sichere WLAN-Netze achten

Man sollte nicht unbedacht auf jeden Zugang zum Internet hüpfen, auch wenn er auf den ersten Blick einladend wirkt und kurzweilige Aktivität verspricht. Insbesondere offene WLAN-Trampoline halten heutigen Sicherheitsanforderungen selten stand: Sie sind oftmals lückenhaft gestrickt und können zu üblen Verletzungen der Privatsphäre führen. Sofern die Benutzung eines unbekannten Hotspots, drahtlosen Heim- oder Firmennetzwerks jedoch unumgänglich ist, sollte das Netz unbedingt mit einer Verschlüsselung gesichert sein – sie garantiert eine sichere Landung beim WLAN-Springen, ohne dass essenzielle Teile durch die Maschen rutschen könnten.



Fraunhofer ACADEMY

3 PASSWORT-AUSDRUCKSTANZ

Ein kurzes starkes Passwort ist besser als ein langes schwaches – und macht häufigen Wechsel überflüssig

Das sportive Gedächtnistraining kombiniert Erkenntnisse aktueller Verschlüsselungsarithmetik mit Grundlagen der klassischen Eurythmie und kann neben alphanumerischen Abfolgen auch Sonderzeichen nonverbal zum Ausdruck bringen. Kreative Interpretationen zunächst kryptisch erscheinender Ziffernfolgen wie ***HksjT1A!*** werden mittels körperlichem Ausdruckstanz zu einprägsamen Passwörtern – wer einmal ***Hanna kauft sich jeden Tag einen Apfel!*** getanzt hat, kann es nie wieder vergessen. Wichtig: Nicht dasselbe Passwort für verschiedene Dienste nutzen!

Fraunhofer ACADEMY

4 ADMIN-FECHTEN

Im Alltag auf Admin-Rechte verzichten

Rein auf die Physiognomie bezogen scheint die Rolle des Administrators beim Fechten viele Vorteile zu bringen: Weitreichende Befugnisse erwecken den Eindruck, sich weitgehend mühelos und effizient vorkämpfen zu können. Tatsächlich aber gibt der Admin durch die schiere Größe seiner Angriffsfläche ein begehrliches Ziel ab – insbesondere in der Arena des World-Wide-Web: Hier können selbst kleine Treffer den potenziell größten Schaden anrichten und sich zu schwerwiegenden und systemweiten Verletzungen ausdehnen. Weitaus besser geschützt hingegen ist der »normale« Benutzer, der mit eingeschränkten Rechten weitaus weniger Angriffsfläche bietet.

5 SELEKTIONS-GOLF

Wichtige Informationen nicht leichtfertig weitergeben

Der Trendsport Selektionsgolf trainiert auf innovative Weise die Einheit zwischen Körper und Geist. Dabei müssen Informationsbälle nicht nur mittels Kombination aus geschmeidiger Bewegung und höchster Konzentration ans Ziel gebracht werden – die zentrale Herausforderung liegt in der exakten Abstimmung des Empfängerkreises auf die weiterzuspielenden Inhalte. Hat man die grundlegenden Regeln einmal verinnerlicht und die Platzreife erreicht, spielt sich Selektionsgolf fast von selbst und schützt ganz nebenbei auch davor, dass sensible Informationen unerwünscht an Dritte weitergespielt werden, nicht zuletzt im Kontext sozialer Netzwerke.

Fraunhofer ACADEMY

6 E-MAIL-KESCHERN

Kritischer Umgang mit E-Mail-Anhängen und Hyperlinks nicht nur unbekannter Absender

Erfolgreiches E-Mail-Keschern ist auch ohne vertiefte Kenntnisse der Phishing-Zoologie möglich. Bereits Anfänger können potenziell schädliche Nachrichten anhand simpler Kriterien identifizieren, die durch die Maschen automatisierter Fangnetze geschlüpft sind – selbst, wenn sie durch trickreiches Mimikry vorgeben, aus dem Freundes- oder Kollegenkreis versandt worden zu sein. Anhängen und Links sollte immer mit Vorsicht begegnet werden, nicht zuletzt in Messenger-Diensten. Eine kurze telefonische Rückfrage beim vermeintlichen Absender schützt effektiv vor unangenehmen Überraschungen.

Fraunhofer ACADEMY

7 INFO-DRACHENFLUG

Durch Information auf dem Laufenden bleiben und den Überblick behalten

Nicht nur die Schönheit weitläufiger Informationslandschaften erschließt sich oftmals erst aus großer Höhe. Auch auf den ersten Blick komplexe Hindernisse können beim Info-Drachenflug mühelos überwunden werden: Der erfahrene Informationsgleiter behält stets die Großwetterlage im Auge und macht sich die Thermik dynamischer Wissensausdehnung zunutze, um entspannt segelnd den Überblick über das große Ganze zu behalten.

Fraunhofer ACADEMY

8 2-FAKTOR-TANDEM

Zwei-Faktor-Authentifizierung nutzen

Das 2-Faktor-Tandem bietet – im Gegensatz zum Solo-Klettern – mit minimal mehr Zeitaufwand einen mindestens doppelten Zugewinn an Sicherheit. Viele Routen zu Online-Diensten können schon heute nur mittels eines zweiten Faktors begangen werden, bei anderen lässt sich die zusätzliche Absicherung immerhin optional einrichten. Dem starken Passwort ***(siehe Passwort-Ausdruckstanz)*** steht dann ein weiterer Code zur Seite, der einmalig und nur zu diesem Zwecke im Moment der Anmeldung generiert und auf ein weiteres Endgerät gesandt wird, bspw. als SMS auf das eigene Mobiltelefon.

Fraunhofer ACADEMY

9 NOTFALL-VERTEIDIGUNG

Notfallplan bereithalten und Ansprechpartner kennen

Um in jeder Situation auf unvorhergesehene Angriffe vorbereitet zu sein, sind ausgeklügelte taktische Handlungsanweisungen vonnöten. Doch auch das stärkste Team muss einen Treffer einstecken können, ohne dadurch aus dem Konzept geworfen zu werden. Dann können exakt auf diese Situationen trainierte Spezialisten das Spiel schnell wieder drehen – aber nur, wenn die gesamte Mannschaft einen Notfallplan einstudiert hat und im Ernstfall sofort an Administratoren oder IT-Sicherheitsbeauftragte übergibt, bspw. bei plötzlichem Angriff auf's eigene Netz oder erfolgreicher Phishing-Taktik des Gegners.

Fraunhofer ACADEMY

10 VERSCHLÜSSELUNGS-STEMMEN

Sensible Informationen nur verschlüsselt übertragen

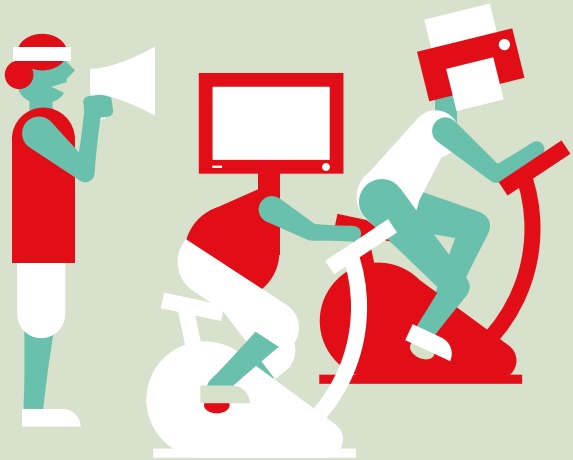
Unbedenkliche Informationen können ohne weiteres per E-Mail versendet werden. Als simple Nachricht birgt die E-Mail allerdings kaum mehr Schutz als eine Postkarte. Sollte der Inhalt nur dem Empfänger zugänglich sein, lohnt sich ein Training im Verschlüsselungs-Stemmen. Es bietet adäquaten Schutz von Ende-zu-Ende und lässt sich ohne großen Aufwand erlernen, um sich vor Massenüberwachung zu schützen und sensible Informationen mit nur wenigen Klicks und doch äußerst effektiv gegen den Zugriff durch Dritte abzusichern.

Fraunhofer ACADEMY

11 UPDATE-TRAINER

Alle Endgeräte regelmäßig auf Aktualisierung überprüfen

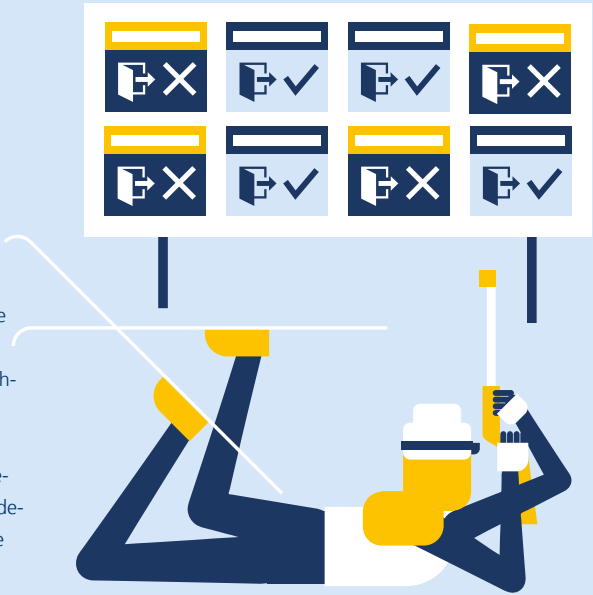
Für die meisten Geräte im Team gehört es zum einstudierten Pflichtprogramm, sich in festen Intervallen unaufgefordert auf den neuesten Stand zu bringen, um aktuellen Sicherheitsanforderungen fit und souverän begegnen zu können. Ein umfassender Trainingsplan sollte aber unbedingt auch Rücksicht auf diejenigen elektronischen Leistungsträger nehmen, deren Updates extern angestoßen werden müssen – dazu zählen Router und Drucker ebenso wie alle Helferlein im Smart Home. Denn nur regelmäßige, manuelle Check-ups und Aktualisierungen können den Erhalt der Leistungsfähigkeit garantieren.



12 LOG-OUT-BIATHLON

Ausloggen nicht vergessen

Der Log-out-Biathlon ist die Königsdisziplin eines langen Bürotags: Nur wer ausreichend geistige Fitness, Konzentration und Ausdauer mitbringt, integriert die Log-out-Routine reibungslos in den Büroalltag und verschließt nach jeder Nutzung alle zugangsbeschränkten Dienste wieder sicher, um sie vor unbefugter Nutzung zu schützen. Der erfahrene Log-out-Biathlet bleibt stets wachsam, lässt selbst bei kurzer Abwesenheit keinen sensiblen Zugang unverschlossen und behält auch auf unbekannten Strecken den Überblick über alle verwendeten Dienste, bspw. bei Anmeldungen über fremde Geräte in Konferenzräumen oder Hotels.



Fraunhofer ACADEMY

Fraunhofer
ACADEMY

Mit den Übungen des IT-Security-Fitness-Kalenders erreichen Sie über ein Jahr hinweg spielerisch die nötige Kondition für das Anforderungs-Terrain im digitalen Arbeitsalltag.

Wenn Sie nach größeren Herausforderungen in Spezial-Sportarten der IT-Sicherheit suchen, probieren Sie sich an den Übungen und Trainings im Lernlabor Cybersicherheit: in kurzen Einheiten üben Sie in Simulationsumgebungen mit fitten Trainern, die Praxiserfahrung und Forschungswissen vereinen. Neben den Basics der IT-Sicherheit trainieren wir auch in Domänen wie Embedded Security, Softwaretesting und IT-Forensik sowie in der IT-Sicherheit für spezielle Branchen wie industrielle Produktion und im Automobilbereich.

Mehr Informationen unter: **www.cybersicherheit.fraunhofer.de**

Fraunhofer
ACADEMY