E-Training – Übersicht VARIANTEN

Online

- Sie verwenden unseren CAMPUS-Bereich https://campus.data-s.de für beliebig viele Teilnehmer - Verwaltung und Betrieb der Plattform sind inklusive und individuell anpassbar!

Inhouse

- Sie bekommen unsere E-Training-Plattform als fertige Appliance bzw. VM zur Einbindung in Ihre IT-Infrastruktur.
- Dabei haben Sie die Möglichkeit, erlerntes Wissen über die Plattform verifizieren zu lassen und Daten direkt an Ihre Personalabteilung zu übermitteln.

Inhalte

- Unsere Inhalte für Ihre bestehenden Plattformen: Sie haben bereits E-Learning oder andere Kollaborations-Plattformen (z. B. Sharepoint) im Einsatz?
- Füllen Sie diese Plattformen mit unseren Inhalten!

DATAS

Stand: 08.03.2017

E-Training – Übersicht LEKTIONEN

Video

- In einem kurzen Video bekommen die Lerner die wichtigsten Inhalte übermittelt, um den Arbeitsalltag in Sachen Datenschutz + Informations-sicherheit optimal bewältigen zu können.
- Nach jeder Lektion werden interaktive Wiederholungs-fragen gestellt, um dem Teilnehmer das Lernen zu erleichtern.

Abschlusstest

- Nachdem die Lektionen ausreichend bearbeitet wurden, kann der Lerner in einem umfassenden Abschlusstest sein Wissen überprüfen.
- Wir definieren die Voraussetzungen für eine ausreichend bearbeitete Lektion individuell nach Ihren Wünschen.

Handout

- War der Abschlusstest erfolgreich, bekommt der Lerner für die Zukunft ein Handout mit an die Hand, in dem er die wichtigsten Inhalte der Lektionen noch einmal nachlesen kann.

Zertifikat

- Am Ende jedes Kurses wird automatisch ein Zertifikat für die Teilnahme erstellt.
- Der Teilnehmer selbst und der Trainer erhalten automatisch eine E-Mail mit dem Zertifikat im Anhang.

DATAS

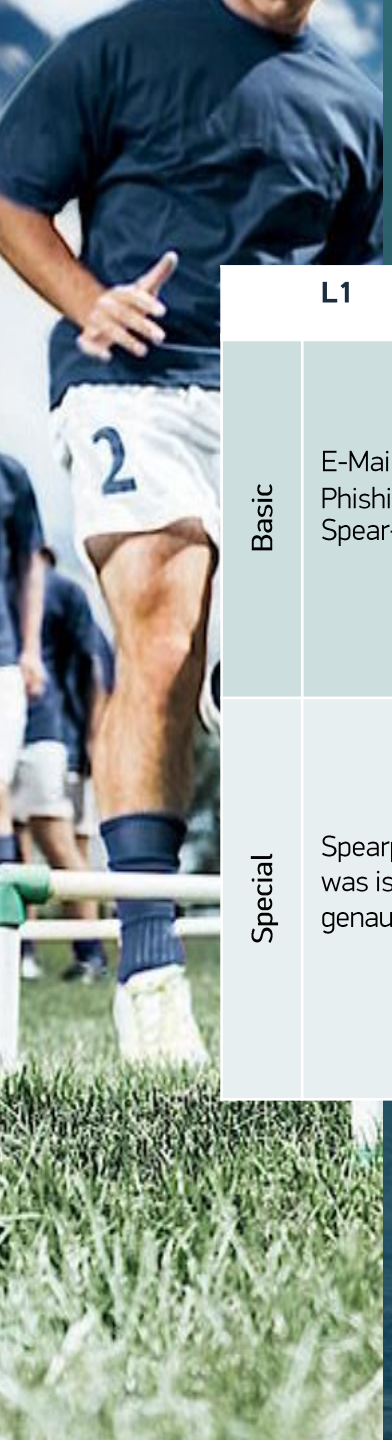
Stand: 08.03.2017

E-Training – Übersicht Security Awareness

	L1	L2	L3	L4	L5	L6	L7	L8	L9	L10
Basic	Schutzziele der Informations-sicherheit	Sicherheit am Arbeitsplatz	Browser-Sicherheit + „drive by“-Malware	Mobile Sicherheit	Social Engineering – ein Überblick	Gefälschte Webseiten	Mein *digitaler Fußabdruck*	Soziale Netzwerke + Cloud	Compliance: Grundlagen	Geschenke + Korruption
Advanced	Phishing und Spear-Phishing gezielt erkennen	Sichere E-Mail	Schutz-klassen	Sicher unterwegs – auf Dienstreise	Umgang mit sensitiven Informationen	Social Engineering: psychologische Hintergründe	Ist WLAN gefährlich?	Keylogger: was ist das?	Und wenn doch was passiert? – Das Notfall-konzept	WhatsApp im Unternehmen
Special	BSI Grundschutz + ISO 27001: was ist das?	Ihr Weg zur ISO 27001-Zertifizierung	Webseiten rechtlich sicher betreiben: Datenschutz und Konformität	Überwachen: aber wie? Gesetzeskonforme Möglichkeiten	Soziale Medien - richtiges Verhalten im Marketing	Der richtige Umgang mit mobilen Datenträgern	Der richtige Umgang mit vertraulichen Dokumenten	Passwort-Safe	*Ihre individuellen Inhalte*	*Ihre individuellen Inhalte*
„Techie“	Phishing und techn. Hinter-gründe	DNS und die Bewahrung der Identität	USB-Ports endlich *geschlossen*?	Social Engineering: "behind the scenes"	Bluetooth und Co: Funken Sie sicher!	Informations-management	Unterwegs: Schutz der Dienst-reisenden	Botnetze und DDOS Angriffe	Sicherheit für Ihr Netzwerk	*Ihre individuellen Inhalte*

DATAS

Stand: 08.03.2017



E-Training – Übersicht Datenschutz

	L1	L2	L3	L4	L5	L6	L7	L8	L9	L10
Basic	E-Mail: Phishing + Spear-Phishing	USB und andere Datenträger	Passwörter – endlich sicher!	Datenschutz – Einführung	Personen-bezogene Daten: Was ist das?	Datenschutzrecht: Verbot mit Erlaubnisvorbehalt	Prinzipien des Daten-schutzes + das Daten-geheimnis	Schutz-maßnahmen	Betroffener + seine Rechte	Sanktionen bei Datenschutz-verstößen und Aufgaben des Datenschutz-beauftragten
Special	Spearphishing – was ist das genau?	Zwei-Faktor-Authentifizierung: Passwortschutz für Fortgeschrittene	Prinzipien des Datenschutzes + das Datengeheimnis (Vollversion)	Datenschutz im Krankenhaus	Datenschutz und Werbung	Datenschutz im Finanzsektor	*Ihre individuellen Inhalte*	*Ihre individuellen Inhalte*	*Ihre individuellen Inhalte*	*Ihre individuellen Inhalte*

DATAS

Stand: 08.03.2017