TRUST IN GERMAN SICHERHEIT

Kursbeschreibungen & Übersicht

G DATA Cyber Defense Awareness Trainings

G DATA CyberDefense AG | Januar 2020

Inhaltsverzeichnis

1. Messung des Basiswissens - Nullmessung

Die Messung des Basiswissens zeigt den aktuellen Wissensstand innerhalb der Organisation an. Sie ist keine Prüfung. Wir erwarten nicht, dass Sie die Messung Ihres Wissensstands fehlerfrei durchlaufen. Die Ergebnisse zeigen, welche Themen mehr Aufmerksamkeit erfordern. Auf diese Weise passen wir die Trainingskurse und Informationen an die bestehenden Bedürfnisse an. Durch die Schulungen bieten wir mehr Informationen zu den Themen.

Die Messung des Basiswissens umfasst die folgenden Themen:

- Datenschutzgrundverordnung (DSGVO)
- Cyber-Sicherheit
- Physische Sicherheit
- Malware
- Phishing
- Risikomanagement

2. Einführungsprogramme

1. **Informationssicherheit**

Technische Maßnahmen sind nur ein Teil für effektive Informationssicherheitspolitik. Ebenso wichtig ist der Umgang der Mitarbeiter mit Unternehmensinformationen. Jeder Mitarbeiter kann von Cyberkriminellen betroffen werden. In diesem Programm folgen Sie 2 Kollegen während eines Arbeitstages. Während eines Arbeitstages werden sie mit Vorfällen konfrontiert, die wir alle aus unserer täglichen Arbeit kennen. Anhand von praktischen Beispielen lernen Sie, wie Sie mit diesen Situationen umgehen.

Nach dem Training können Sie die folgenden Fragen beantworten:

- Wie gehen Sie mit Informationen sorgfältig um?
- Was tun Sie, wenn Sie eine verdächtige Situation bemerken?
- Wie gehen Sie sicher mit Passwörtern um?
- Was sind die Regeln für einen aufgeräumten Schreibtisch, ein aufgeräumtes Büro und einen gesperrten Bildschirm?
- Wie gehen Sie mit Besuchern um?
- Woran erkennt man verdächtige E-Mails?
- Wie kann man sensible Informationen sicher ausdrucken?
- Wofür nutzen Sie ein Virtual Private Network (VPN)?
- Wie kann man in der Öffentlichkeit sicher arbeiten?

2. Cyber-Sicherheit für Führungskräfte

Management und Vorstand spielen eine entscheidende Rolle beim Schutz von Informationen. In diesem Einführungskurs erfahren Sie nicht nur, warum Cyber-Sicherheit wichtig ist und wie Sie mit Cyber-Risiken umgehen, sondern erhalten auch praktische Tipps zum Schutz des Unternehmens vor Cyber-Bedrohungen. Nach Abschluss dieser Schulung können Sie einen eigenen Plan erstellen, mit dem Sie sofort loslegen können.

Nach dem Training können Sie die folgenden Fragen beantworten:

- Was ist Cyber-Sicherheit?
- Warum ist Cyber-Sicherheit wichtig?
- Welche Cyber-Angriffe richten sich direkt an Management und Vorstand?
- Wie wichtig ist die Cyber-Sicherheit für Ihr Unternehmen?
- Welche Maßnahmen benötigt Ihre Organisation?
- Wie arbeiten Sie in Ihrem Unternehmen an der Cyber-Sicherheit?
- Was tun Sie bei einem Vorfall?

3. Security Awareness für IT-Professionals

IT-Experten nutzen ihr Wissen und ihre Fähigkeiten, um die Sicherheit von Informationssystemen zu gewährleisten. Deshalb ist es gut, dass Sie als IT-Profi die Sicherheitsrisiken in Ihrem Unternehmen kennen. Diese Einführung deckt die häufigsten Sicherheitsrisiken ab und vermittelt Ihnen, wie Sie diese managen können. Auf diese Weise tragen Sie als IT-Profi dazu bei, die Informationssicherheit in Ihrer Organisation zu optimieren.

Nach dem Training können Sie die folgenden Fragen beantworten:

- Woraus besteht ein Benutzerkonto?
- Welche Risiken bestehen bei der Verwendung von Administratorkonten in Ihrem Unternehmen?
- Was bringt die Verwendung von Datenmanagement?
- Worauf achten Sie bei der Auswahl eines Cloud-Services?
- Welche Risiken bestehen bei einigen gängigen Methoden des Datenaustauschs?
- Wie können Sie Bring Your Own Device (BYOD) in Ihrem Unternehmen so sicher wie möglich implementieren?
- Wie arbeiten Cyber-Kriminelle?

3. Vertiefungsprogramme

1. Phishing

In diesem Training lernen Sie, wie Sie einen Phishing-Angriff erkennen und melden können. Jeden Tag versuchen Kriminelle, vertrauliche Informationen zu stehlen, indem sie Social Engineering und andere Formen der Täuschung einsetzen. Vergewissern Sie sich also, dass Sie sich bewusst sind, wenn jemand versucht, Sie zu täuschen. Dieses Training lehrt Sie, besonders auf Links zu achten und welche Informationen Sie teilen. Auf diese Weise schützen Sie sich und Ihr Unternehmen vor Phishern.

Nach dem Training können Sie die folgenden Fragen beantworten:

- Was ist Phishing?
- Wie arbeiten Phisher und wie erkenne ich sie?
- Wie kann man verhindern, dass man Opfer von Phishing wird?

2. Cyber-Sicherheit

In dieser Schulung lernen Sie die Wichtigkeit von Risiken und Cyber-Sicherheit kennen. Sie begleiten Rosa bei der Arbeit und sehen, wie sie die Sicherheit digitaler Informationen schützt. Sie erfahren, welche Maßnahmen Sie bei Ihrer täglichen Arbeit zum Schutz der Sicherheit digitaler Informationen ergreifen können.

Nach dem Training können Sie die folgenden Fragen beantworten:

- Was ist Cyber-Sicherheit?
- Wie erkennen Sie eine Phishing-E-Mail und wie reagieren Sie darauf?
- Wie schützen Sie Login-Daten und Konten?
- Wie kann man Informationen sicher speichern?
- Was ist das Internet der Dinge und wie gehen Sie sicher damit um?
- Wie kann man das Internet sicher nutzen?
- Wie verhindert man, dass man Opfer von Social engineering wird?

3. Arbeiten in der Cloud

Mit der Cloud können Sie jederzeit und überall auf Informationen zugreifen. Sie bietet große Chancen, hat aber auch Risiken. Sie können die Vorteile der Cloud besser nutzen, wenn Sie wissen, wie man sie benutzt. In dieser Schulung lernen Sie alles Notwendige, um sicher in der Cloud zu arbeiten.

Nach dem Training können Sie die folgenden Fragen beantworten:

- Was ist „in der Cloud arbeiten‘‘?
- Was ist ein öffentlicher Cloud-Dienst und woraus bestehen die Vor- und Nachteile?
- Was ist ein privater Cloud-Dienst und woraus bestehen die Vor- und Nachteile?
- Wie arbeiten Sie sicher in der Cloud?

4. Klassifizierung von Informationen

Die Arbeit mit Informationen ist ein wichtiger und großer Teil eines Unternehmens. Daher ist es wichtig, dass Sie Informationen korrekt klassifizieren. Daraus ergibt sich, welches Schutzniveau erforderlich ist. Jeder weiß dann, welches Maß an Vertraulichkeit, Integrität und Verfügbarkeit er bei der Arbeit mit Informationen anwenden sollte. Damit soll sichergestellt werden, dass Informationen nicht verloren gehen oder in die falschen Hände gelangen.

Nach dem Training können Sie die folgenden Fragen beantworten:

- Was ist eine Klassifizierung von Informationen?
- Warum ist es wichtig?
- Wie klassifizieren Sie Informationen?
- Wie gehen Sie mit klassifizierten Informationen um?

5. Social Engineering

Ein Social Engineer manipuliert das schwächste Glied in der Informationssicherheit: den Menschen. Er versucht auf verschiedene Weise, auf Informationen zuzugreifen, um sie zu ändern oder für kriminelle Zwecke zu verwenden. In dieser Schulung lernen Sie, wie ein Social Engineer arbeitet und wie Sie einen Social engineering Angriff erkennen.

Nach dem Training können Sie die folgenden Fragen beantworten:

- Was ist Social Engineering?
- Welche Eigenschaften hat ein Social Engineering Angriff?
- Wie schützt man sich vor einem Social Engineering Angriff?

6. Moderne Arbeitswelten

Heutzutage können Sie jederzeit und überall arbeiten: zu Hause, in der Öffentlichkeit oder an flexiblen Arbeitsplätzen: wo immer Sie wollen. Aber diese Art der flexiblen Arbeitsweise ist nicht ohne Informationssicherheitsrisiken möglich. In diesem Training wird erklärt, wie Sie auch außerhalb des Büros optimal und sicher arbeiten können.

Nach dem Training können Sie die folgenden Fragen beantworten:

- Was ist die moderne Arbeitsweise?
- Wie arbeiten Sie sicher zu Hause, in der Öffentlichkeit und an flexiblen Arbeitsplätzen?

7. Malware

Malware steht für „bösartige Software". Es ist ein Sammelbegriff für verschiedene Arten von bösartiger Software. Ransomware ist eine bekannte Form von Malware.

Malware kann in einem Unternehmen zu erheblichen Schäden führen. So können beispielsweise personenbezogene Daten gestohlen oder sensible Informationen an die Öffentlichkeit gebracht werden. Diese Schulung stellt sicher, dass Sie sich der Gefahren der verschiedenen Formen von Malware bewusst sind. Sie lernen, Malware zu erkennen und Infektionen zu verhindern.

Nach dem Training können Sie die folgenden Fragen beantworten:

- Was ist Malware?
- Welche Formen von Malware gibt es?
- Was macht Malware?
- Wie kann man Malware erkennen?
- Wie können Sie Malware verhindern?

8. Mobile Geräte

Was haben Sie auf Ihrem Smartphone, Laptop oder Tablet gespeichert? Es sind nicht nur Ihre persönlichen Daten. Möglicherweise haben Sie auch sensible Geschäftsdaten gespeichert. Dies kann zu schwerwiegenden Folgen führen, wenn es in die falschen Hände gerät. Viele von uns haben diese Möglichkeit nie in Betracht gezogen. Wir wissen auch nicht immer, was wir in dieser Situation tun sollen. In dieser Schulung lernen Sie, wie Sie den Verlust Ihrer Arbeitsmittel verhindern und sicher arbeiten können.

Nach dem Training können Sie die folgenden Fragen beantworten:

- Inwiefern werden mobile Geräte eingesetzt?
- Welche Risiken bestehen bei der Nutzung mobiler Geräte?
- Wie können Sie diese Risiken begrenzen?
- Was ist zu tun, wenn es einen Vorfall gibt?

9. Risikomanagement

In dieser Schulung lernen Sie, was Risikomanagement ist, welche Risiken Sie eingehen können und welche Rolle Sie dabei spielen. Die Schulung wurde für (Projekt-) Manager entwickelt, aber auch andere Mitarbeiter sollten die Schulung belegen, um zu lernen, wie man besser mit Risiken umgeht. Sie entdecken die Rolle des Risikomanagers innerhalb des Unternehmens, lernen die Darstellung von Risiken durch eine Selbsteinschätzung kennen und erfahren, wann Sie den Risikomanager um Rat oder Unterstützung bitten sollten.

Nach dem Training können Sie die folgenden Fragen beantworten:

- Was ist der Zweck des Risikomanagements?
- Welche Rolle spielt der Risikomanager?
- Was ist ein Risiko?
- Wie identifizieren Sie Risiken?
- Was sind die Folgen von Risiken?
- Welche Kontrollmaßnahmen können Sie ergreifen?
- Wann wenden Sie sich für Rat und Tat an den Risikomanager?

10. EU Datenschutzgrundverordnung (EU-DSGVO)

Seit dem 25. Mai 2018 ist die Datenschutzgrundverordnung, kurz DSGVO, in Kraft. Seitdem kann jeder die Unternehmen für die Einhaltung dieser neuen europäischen Datenschutzgesetze verantwortlich machen. In dieser Schulung lernen Sie die wichtigsten Merkmale der DSGVO kennen und erfahren, wie Sie personenbezogene Daten schützen, verarbeiten und speichern können.

Nach dem Training können Sie die folgenden Fragen beantworten:

- Was ist die EU-DSGVO?
- Was sind personenbezogene Daten?
- Was beinhaltet die Verarbeitung personenbezogener Daten?
- Warum ist ein guter Schutz personenbezogener Daten wichtig?
- Was sind die Grundregeln der EU-DSGVO?
- Welche Rechte haben die betroffenen Personen?
- Was sind die Aufgaben und Verantwortlichkeiten bei der Verarbeitung?
- Was sollten Sie tun, um personenbezogene Daten zu schützen?

11. Physische Sicherheit

Physische Sicherheit schützt Menschen, Vermögenswerte und Informationen eines Unternehmens. Außer der technischen Sicherheit benötigen Informationen auch physische Sicherheit. Die wichtigsten Bedrohungen, vor denen die physische Sicherheit ein Unternehmen schützt, sind absichtliche Bedrohungen durch Personen. Denken Sie an Diebstahl und unbefugten Zugriff. In diesem Training erfahren Sie, welche Maßnahmen ein Unternehmen zur physischen Sicherheit ergreifen kann und welche Rolle Sie dabei spielen.

Nach dem Training können Sie die folgenden Fragen beantworten:

- Was ist physische Sicherheit?
- Warum ist die physische Sicherheit wichtig?
- Wie tragen Sie selbst zur physischen Sicherheit bei?

4. Microlearning

1. Verwendung von Passwörtern

Die Sicherheitsrichtlinie beginnt mit einem guten Passwort. Sichere Passwörter verhindern den unbefugten Zugriff auf sensible Informationen. In wenigen Minuten erklärt Ihnen dieses Mircolearning, welche Risiken es bei der Verwendung von Passwörtern gibt; und es zeigt Ihnen, wie Sie ein starkes, leicht zu merkendes Passwort erstellen können.

Nach dem Training können Sie die folgenden Fragen beantworten:

- Wie erstellt man sichere Passwörter, die leichter zu merken sind?
- Wie kann man all seine verschiedenen Passwörter sicher verwalten?

2. Außerhalb des Büros sicher arbeiten

Die Arbeit außerhalb des Büros unterscheidet sich von der Arbeit im Büro. Außerhalb des Büros arbeiten Sie mit mobilen Geräten und haben nicht unbedingt eine sichere Internetverbindung. Dieses Mircolearning vermittelt Ihnen in ca. 3 Minuten, wie Sie außerhalb des Büros ohne Risiken optimal arbeiten können.

Nach dem Training können Sie die folgenden Fragen beantworten:

- Wie arbeitet man sicher mit sensiblen Geschäftsinformationen?
- Was macht man mit Geräten, wenn man sie nicht benutzt?
- Wie gehen Sie sicher mit mobilen Geräten um?
- Was machen Sie mit Dokumenten, die nicht mehr benötigte, sensible Informationen enthalten?
- Wie kann man auf sichere Weise drucken?
- Wie kann man sensible Informationen auf sichere Weise versenden?

3. Sichern Sie Ihre mobilen Geräte

Mobile Geräte sind immer in Reichweite. Es gibt viele Vorteile, aber einige von ihnen bergen Risiken. Wenn Sie sich dieser Risiken bewusst sind, wissen Sie auch, wie Sie sich davor schützen können. Dieses Mircolearning erklärt, warum das Sichern mobiler Geräte wichtig ist.

Nach dem Training können Sie die folgenden Fragen beantworten:

- Wie sichern Sie alle Ihre mobilen Geräte auf die richtige Weise?
- Welche Risiken bestehen bei der Nutzung mobiler Geräte?

4. Vergewissern Sie sich, mit wem Sie es zu tun haben

Social-Engineers präsentieren sich als eine andere Person. Dies geschieht per E-Mail, beim Telefonieren oder sogar persönlich. Aber wie findet man heraus, mit wem man es zu tun hat? Wie verhindert man, dass man Opfer von Social engineering wird? Wenn Sie einen Social-Engineer erkennen, dann geben Sie keine Informationen an diese falsche Person. Dieses Microlearning zeigt Ihnen in wenigen Minuten, wie Sie herausfinden, mit wem Sie es zu tun haben und lehrt Sie, wie Sie mit verdächtigen Situationen umgehen.

Nach dem Training können Sie die folgenden Fragen beantworten:

- Wie erhalten böswillige Personen sensible Informationen?
- Wie stellen Sie sicher, dass Sie Informationen nur mit den richtigen Personen teilen?

5. Melden von Sicherheitsvorfällen

Jeder in einem Unternehmen kann mit einem Vorfall der Informationssicherheit konfrontiert werden. Ergreifen Sie immer sofort Maßnahmen, wenn Sie das Gefühl haben, dass etwas nicht stimmt und melden Sie Vorfälle. Auf diese Weise stellen Sie sicher, dass Ihr Unternehmen schnell handeln kann. Dieses Microlearning zeigt, was ein Informationssicherheitsvorfall ist und wie man auf einen solchen Vorfall reagiert.

Nach dem Training können Sie die folgenden Fragen beantworten:

- Was sollen Sie tun, wenn Sie etwas Seltsames bemerken?
- Was sollten Sie tun, wenn Sie feststellen, dass Vermögenswerte verschwunden sind?
- Wie können Sie Vorfälle im Bereich der Informationssicherheit verhindern?

6. Wie müssen Informationen klassifiziert werden?

Die Arbeit mit Informationen ist ein wichtiger Teil jedes Unternehmens. Die korrekte Klassifizierung von Informationen zeigt das erforderliche Schutzniveau an. Jeder weiß dann, welches Maß an Vertraulichkeit, Integrität und Verfügbarkeit er bei der Arbeit mit den Informationen anwenden sollte. Damit soll sichergestellt werden, dass Informationen nicht verloren gehen oder in falsche Hände gelangen. In diesem Mircolearning erfahren Sie, warum die Klassifizierung von Informationen für Ihr Unternehmen wichtig ist.

Nach dem Training können Sie die folgenden Fragen beantworten:

- Warum ist es wichtig, Informationen richtig zu klassifizieren?
- Welche sind die gängigsten Klassifizierungskategorien?
- Welche Risiken bestehen beim Verlust bestimmter vertraulicher Informationen?

Wie verhält man sich, wenn Menschen nach sensiblen Informationen fragen?

7. Internet of Things (IoT)

Es gibt immer mehr „intelligente" Geräte, die über das Internet ein Netzwerk bilden, wie beispielsweise intelligente Uhren und externe Festplatten. Viele dieser Geräte sind nicht ausreichend geschützt. Hacker oder infizierte „intelligente" Geräte stellen eine Bedrohung für geschäftliche Geräte dar. Es ist oft unklar, wer innerhalb des Unternehmens für den Schutz dieser „intelligenten" Geräte verantwortlich ist. In diesem Microlearning lernen Sie, wie Sie mit IoT-Geräten so sicher wie möglich arbeiten.

Nach dem Training können Sie die folgenden Fragen beantworten:

- Was ist das IoT?
- Wie infizieren IoT-Geräte Firmengeräte?
- Welche Risiken birgt das IoT?
- Wie gehen Sie mit den Schwächen des IoT um?

8. Ransomware

Ransomware ist eine bekannte Form von Malware und wird oft in den Nachrichten erwähnt. Bei Ransomware bittet Sie jemand um Zahlung eines Lösegelds, um eine Blockade von einem Computer oder Computersystem zu beseitigen. Man weiß nur nie sicher, ob die Blockade auch nach der Bezahlung verschwindet. Es ist besser, die Wahrscheinlichkeit von Ransomware zu reduzieren. In dieser Schulung lernen Sie, wie Sie das Risiko von Ransomware minimieren können.

Nach dem Training können Sie die folgenden Fragen beantworten:

- Was ist Ransomware?
- Wie reduziert man das Risiko von Ransomware?

9. Datenschutz in der Praxis

Seit dem 25. Mai 2018 ist die Datenschutzgrundverordnung, kurz DSGVO, in Kraft. Seitdem können Organisationen von allen Betroffenen für die Einhaltung dieser neuen europäischen Datenschutzgesetze verantwortlich gemacht werden. In diesem Training lernen Sie, wie Sie DSGVO anhand erkennbarer praktischer Situationen anwenden.

Nach dem Training können Sie die folgenden Fragen beantworten:

- Was sind (besondere) personenbezogene Daten?
- Warum ist der Schutz personenbezogener Daten wichtig?
- Wie gehen Sie in der Praxis mit Datenschutz um?

5. Security Flashes

1. Bring your own device

Wenn Mitarbeiter ihre eigenen mobilen Geräte für geschäftliche Zwecke nutzen können, profitiert auch Ihr Unternehmen davon: zum Beispiel durch geringere Service- und Hardwarekosten. Darüber hinaus verfügen die Mitarbeiter oft über Smartphones, Tablets und Laptops, die intelligenter, besser und schneller sind als die Firmengeräte. In diesem Aufklärungsvideo erfahren Sie, wie Sie Ihre eigene Ausrüstung für Ihre Arbeit verwenden, was die Gefahren sind und wie Sie mit Vorfällen umgehen.

Nach dem Video können Sie die folgenden Fragen beantworten:

- Wie können Sie Ihr eigenes Gerät für geschäftliche Zwecke nutzen?
- Welche Gefahren bestehen bei der Arbeit mit eigenen Geräten?
- Wie können Sie diese Gefahren vermeiden?
- Was ist im Falle eines Sicherheitsvorfalles zu tun?

2. Schreibtisch und Büro aufgeräumt und Bildschirm gesperrt

Man weiß nie, wer an seinem Schreibtisch vorbeigeht, wenn man nicht da ist. Lassen Sie daher sensible Informationen nicht unbeaufsichtigt. Dies gilt sowohl für die Informationen auf Ihrem Bildschirm als auch auf Ihrem Schreibtisch. Sperren Sie Ihren Computer und lassen Sie keine sensiblen Informationen zurück, wenn Sie Ihren Arbeitsplatz verlassen. Nicht einmal, wenn Sie nur für einen Moment weg sind. In etwas mehr als einer Minute erfahren Sie, warum eine klare Schreibtisch-, Bildschirm- und Bürorichtlinie zu einer sicheren Organisation beiträgt.

Nach dem Video können Sie die folgenden Fragen beantworten:

- Warum sollten Sie Ihren Arbeitsplatz aufgeräumt und ordentlich halten?
- Was sind die Gefahren, wenn Sie das nicht tun?
- Wie vermeiden Sie diese Gefahren?

3. Phishing

Phishing ist heute eine der größten Bedrohungen der Cyber-Kriminalität. Es gibt viele Formen des Social engineering, aber Phishing ist bei weitem die bekannteste und erfolgreichste. Die Idee ist einfach: Nachdem Sie auf einen falschen Link klicken oder eine Anlage öffnen, hat der Cyber-Kriminelle Zugriff auf Ihre Daten. Dieses Aufklärungsvideo zeigt Ihnen, wie Sie verdächtige E-Mails erkennen können, was die Gefahren sind und was Sie tun müssen, wenn etwas schiefgeht.

Nach dem Video können Sie die folgenden Fragen beantworten:

- Was suchen Phishing-Kriminelle?
- Woran erkennt man eine Phishing-E-Mail?
- Was tun Sie, wenn Sie einem Link oder einer Anlage nicht vertrauen?

4. Sicherheitsvorfälle melden

Sicherheitsrisiken treten täglich in Ihrem Unternehmen auf. Auf den ersten Blick scheinen sie kaum aufzufallen, aber diese Risiken können zu Vorfällen führen. Wenn Sie denken, dass es einen Vorfall oder ein verdächtiges Verhalten gibt, sollten Sie Maßnahmen ergreifen. Ihre Organisation wird dann die richtigen Sicherheitsmaßnahmen ergreifen. Dieses Aufklärungsvideo zeigt Ihnen, wie Sie Vorfälle verhindern und mit verdächtigen Situationen umgehen können.

Nach dem Video können Sie die folgenden Fragen beantworten:

- Was genau ist ein Sicherheitsvorfall?
- Was genau sollten Sie tun, wenn Sie mit einem Vorfall zu tun haben?
- Was können Sie noch tun, um die Sicherheit von Informationen zu gewährleisten?

5. Starke Passwörter

Wir alle wissen, dass wir sichere Passwörter verwenden müssen, denn schwache Passwörter sind leicht zu knacken. Sobald ein Cyber-Krimineller ein Passwort hat, hat er Zugang zu vertraulichen Informationen. Dieses Video zeigt Ihnen, wie Sie sichere Passwörter erstellen, was die Gefahren eines schwachen Passworts sind und wie Sie mit Ihren Passwörtern sicher umgehen.

Nach dem Video können Sie die folgenden Fragen beantworten:

- Was ist ein starkes Passwort?
- Wie stellen Sie sicher, dass Ihr Passwort leicht zu merken, aber schwer zu erraten ist?

6. Arbeiten in der Öffentlichkeit

Flexible Arbeit wird immer beliebter. Immer mehr Mitarbeiter arbeiten von überall aus und wann sie wollen: von Zuhause, im Büro, im Zug oder im öffentlichen Raum. Aber die Arbeit in der Öffentlichkeit bringt verschiedene Sicherheitsrisiken mit sich. Dieses Aufklärungsvideo zeigt Ihnen in weniger als 2 Minuten, wie Sie die Vorteile der Arbeit in der Öffentlichkeit voll ausschöpfen können, ohne das Risiko sensible oder vertrauliche Informationen zu verraten.

Nach dem Video können Sie die folgenden Fragen beantworten:

- Worauf achten Sie bei der Arbeit in der Öffentlichkeit?
- Worauf achten Sie bei der Nutzung von sozialen Medien?

7. Social Engineering

Social engineering ist eine Technik, bei der jemand versucht, vertrauliche Daten zu stehlen, indem er das „Opfer" manipuliert. Sie arbeiten mit vielen Informationen, die für andere attraktiv sind. Es ist daher wichtig, dass Sie die Arbeitsweise von Social-Engineers erkennen. Seien Sie zum Beispiel immer vorsichtig, welche Art von Informationen Sie in der Öffentlichkeit diskutieren. Wenn Sie sensible Informationen in der Öffentlichkeit besprechen, können andere davon erfahren. Dies kann unangenehme Folgen haben.

Nach dem Video können Sie die folgenden Fragen beantworten:

- Was ist der Zweck von Social engineering?
- Worauf sollten Sie bei einem geschäftlichen Gespräch in der Öffentlichkeit achten?
- Was ist zu tun, wenn eine unbekannte Person um Informationen bittet?

8. Zutrittskontrolle

Dieses Video zeigt, warum die Zutrittskontrolle für die Informationssicherheit wichtig ist. Die Verwendung eines Zutrittsausweises erhöht die Sicherheit eines Gebäudes, da nur Personen mit einem Zutrittsausweis direkten Zugang haben. Außerdem gibt dieses System einen Einblick, wer sich im Gebäude befindet. Im Falle von Katastrophen ist dies eine wichtige Information. Melden Sie daher jeden Verlust Ihres Ausweises unverzüglich der zuständigen Person oder Abteilung.

Nach dem Video können Sie die folgenden Fragen beantworten:

- Was sollten Sie mit Ihrem Zutrittsausweis machen?
- Wie gehen Sie mit Besuchern um?

9. Soziale Medien & Arbeiten in der Cloud

Soziale Medien ermöglicht es Ihnen, ein großes Publikum zu erreichen, aber es ist auch eine Quelle von Identitätsdiebstahl. Cloud-Dienste sind sehr zugänglich, aber bei einigen Cloud-Diensten hat der Service-Anbieter die gleichen Zugriffsrechte auf Ihre Informationen wie Sie. Um zu verhindern, dass dies unangenehme Folgen für Sie und Ihre Organisation hat, wird Ihnen dieses Aufklärungsvideo die Risiken der Nutzung von sozialen Medien und der Cloud aufzeigen.

Nach dem Video können Sie die folgenden Fragen beantworten:

- Welche Art von Informationen können Sie sicher über soziale Medien teilen und welche nicht?
- Welche Risiken bestehen beim Informationsaustausch über einen Cloud-Service?
- Wie können Sie die Vorfälle verhindern?

10. Klassifizierung von Informationen

Die Arbeit mit Informationen ist ein wichtiger Teil eines Unternehmens. Die korrekte Klassifizierung von Informationen zeigt das erforderliche Schutzniveau an. Jeder weiß dann, welches Maß an Vertraulichkeit, Integrität und Verfügbarkeit er bei der Arbeit mit den Informationen anwenden sollte. Damit soll sichergestellt werden, dass Informationen nicht verloren gehen oder in die falschen Hände gelangen. Dieses Aufklärungsvideo erklärt, warum es wichtig ist, jede Information richtig zu klassifizieren.

Nach dem Video können Sie die folgenden Fragen beantworten:

- Warum ist es wichtig, Informationen richtig zu klassifizieren?
- Welche sind die gängigsten Klassifizierungskategorien?
- Welche Gefahren bestehen beim Verlust von Informationen einer bestimmten Art von Klassifizierung?
- Was ist zu tun, wenn Menschen um Informationen bitten?

11. Malware

Malware steht für „bösartige Software". Es ist ein Sammelbegriff für verschiedene Arten von schädlicher Software. Malware kann in einem Unternehmen zu erheblichen Schäden führen. In diesem Video erfahren Sie, welche Signale Sie erkennen und was Sie tun müssen, wenn Sie denken, dass Sie an Malware leiden.

Nach dem Video können Sie die folgenden Fragen beantworten:

- Was ist Malware?
- Was macht Malware?
- Was sind die Anzeichen von Malware?