Lerneinheit

Abschließende Einheit

Projekt: B-SAFE
Nummer: 2018-1CZ01-KA204-048148

Funded by the
Erasmus+ Programme
of the European Union

Co-funded by the
Erasmus+ Programme
of the European Union

1. Die zehn größten Internet-Bedrohungen für Benutzer

Der Zugang zum Internet ist in diesem digitalen Zeitalter einfach, und es bietet viele Möglichkeiten, die virtuelle Welt zu erkunden, in der im Gegensatz zur realen Welt alles leicht zugänglich ist. Es eröffnet eine neue Welt und bringt viele Vorteile, aber auch viele Risiken mit sich.

1. Ungeeigneter Inhalt

Es gibt Tonnen von Inhalten im Internet, und nicht alle diese Inhalte sind gesellschaftlich akzeptabel, noch sind sie nach Alter oder Gebiet klassifiziert. Einige Inhalte können illegal, unangemessen, beleidigend oder für bestimmte Altersgruppen ungeeignet sein. Jeder kann unangemessene, beunruhigende oder explizite Inhalte finden, sogar kleine Kinder ohne Aufsicht.

Viele störende Websites sind nicht "illegal", was bedeutet, dass niemand ihren Inhalt überwacht und verwaltet. Bei einigen dieser Inhalte handelt es sich um Pornographie, Gewalt, gefährliche Produkte (wie Waffen), Rassismus oder Hass, Pro-Ana-Sites (die Magersucht fördern) oder andere Websites mit extremistischen Inhalten.

2. Datenklau

Finanzielle oder persönliche Informationen werden durch die Verwendung von Computern, Servern und anderen elektronischen Geräten gestohlen, um einen Nutzen oder Schaden für den bzw. die Betroffene zu erzielen. Cyber-Diebe können Banken, Unternehmen und Einzelpersonen ins Visier nehmen. Es ist eine illegale Handlung zur Erlangung sensibler Daten, zu denen auch unverschlüsselte Kreditkartennummern, Bankkontodaten von Einzelpersonen, Passwörter, in Unternehmen gespeicherte Informationen, Geschäftsgeheimnisse, geistiges Eigentum, Quellcode, Kundeninformationen oder Mitarbeiterdaten gehören.

Der bzw. die Cyberkriminelle kann auf die Computer dieser BenutzerInnen über Spyware zugreifen, eine Software, die es einem Nutzenden ermöglicht, Informationen über die Computeraktivitäten eines anderen zu erhalten.

3. Identitätsdiebstahl

Identitätsdiebstahl ist der Akt des Diebstahls persönlicher Identifikationsdaten, um illegale Handlungen zu begehen.

In der ersten Phase erwirbt der bzw. die TäterIn eine fremde Computer-Identität. Dies geschieht meist durch Diebstahl elektronischer Daten (Passwörter, Zugangsdaten usw.), meist durch unbefugtes Kopieren (Skimming), betrügerisches Phishing oder Hacking.

In der zweiten Phase missbraucht der bzw. die TäterIn die Identität zum eigenen Vorteil, um dem Opfer zu schaden. Zum Beispiel indem unter dem Namen des Opfers in sozialen Netzwerken wie Facebook gehandelt wird. Es ist der Akt des Diebstahls persönlicher Identifikationsinformationen, um illegale Handlungen zu begehen, wie z.B.: Eröffnung einer Kreditlinie, Anmietung eines Hauses, Kauf von Waren oder Dienstleistungen, Auktions- und Lohnbetrug oder Erpressung.

4. Unerwünschte Aufmerksamkeit

Diese Art von Aufmerksamkeit könnte von jemandem kommen, der einfach von dem Opfer besessen ist (Cyberstalking) oder von jemandem, dessen Absicht es ist, dem Opfer zu schaden (Cyberbullying).

Einerseits ist Cyberstalking eine unerwünschte, zwanghafte Aufmerksamkeit gegenüber einer bestimmten Person über das Internet. Es wird über Online-Technologien wie E-Mail, soziale Netzwerke, Instant Messaging, online verfügbare persönliche Daten begangen - alles im Internet kann von Cyberstalkern dazu benutzt werden, unangemessenen Kontakt mit ihren Opfern aufzunehmen. Einige Möglichkeiten sind, der Person online zu folgen, aufdringlich nach persönlichen Daten zu suchen, heimlich online zu beobachten, hartnäckig anzurufen und zu simsen, um sie zu manipulieren, und verschiedene andere Mittel, um sich dem Opfer unerwartet zu nähern.

Auf der anderen Seite ist Cybermobbing ein Verbrechen, das dann auftritt, wenn Menschen soziale Medien oder das Internet benutzen, um andere einzuschüchtern, zu belästigen, zu bedrohen oder herabzusetzen.

5. Betrügereien und Tricks

Eine Art von Betrug oder Trick wäre Phishing. Dabei handelt es sich um eine Praxis des Versendens betrügerischer Mitteilungen, die scheinbar aus einer vertrauenswürdigen Quelle stammen, in der Regel per E-Mail.

Diese Mitteilungen können Malware (Spyware, Lösegeld, Viren und Würmer) enthalten, was normalerweise durch gefährliche Klicks oder E-Mail-Anhänge geschieht, die dann riskante Softwares installieren.

6. Unerwünschte Informationen

Über das Internet können wir am Ende Informationen finden, die wir nicht gesucht haben, oder falsche Informationen oder Profile. **Sie können irreführende Informationen finden, entweder anstelle von dem, was Sie gesucht haben, oder ohne zu fragen**.

Das beliebteste Online-Kommunikationsmedium ist die E-Mail. Es ist in unserer täglichen Routine sehr verbreitet, und deshalb ist es eines der beliebtesten Medien für Spam. Gefälschte E-Mails sind eine häufige Bedrohung, aber Sie können diese Art von irreführender Information auch über Nachrichten in sozialen Netzwerken oder auf verschiedenen Websites erhalten.

Darüber hinaus sind gefälschte Nachrichten überall zu finden, nicht nur bei der Benutzung der E-Mail. In sozialen Netzwerken findet man nicht nur gefälschte Nachrichten, sondern auch gefälschte Identitäten.

7. Leichte Ausbreitung und lange Verweildauer

Informationen wie Fotos, Nachrichten usw. können jederzeit, überall und von jedermann hochgeladen werden. Wenn die Informationen einmal online sind, bleiben sie für immer erhalten, so dass Sie mit den Informationen, die Sie online weitergeben, sehr vorsichtig umgehen müssen.

Es ist auch sehr einfach, sie in kurzer Zeit auf der ganzen Welt zu verbreiten.

8. Vernichtung oder Änderung von Daten

Wichtige Daten können auf dem Computer des Nutzenden zerstört oder verändert werden, um Schaden anzurichten.

Eine Möglichkeit könnten Viren sein, d.h. Computerprogramme, die andere Computerprogramme infizieren, wichtige Systemdaten zerstören und Netzwerke funktionsunfähig machen. Ein anderes Beispiel könnten Trojaner sein, d.h. Computerprogramme, die sich Zugang zu einem Computer oder System verschaffen, das in Form von normaler Software getarnt ist, um Systemprozesse, Festplattendaten usw. zu schädigen.

9. Deaktivieren des Geräts

Das Betriebssystemgerät des Computers kann von einem Trojaner angegriffen werden. Es handelt sich dabei um ein Computerprogramm, das Zugriff auf einen Computer oder ein System erhält.

Trojaner werden in Form von normaler Software getarnt, um Systemprozesse, Festplattendaten usw. zu beschädigen. Meist werden sie über E-Mail-Anhänge eingeführt.

10. Cyber-Terrorismus

Cyber-Terrorismus ist immer gravierender als andere Verhaltensweisen, die im oder durch den Cyberspace ausgeführt werden.

Diese Art von Verbrechen ist ein Cyberattack, der darauf abzielt, Angst zu erzeugen oder die Gesellschaft mit einem ideologischen Ziel einzuschüchtern. Zu diesem Zweck benutzt der Terrorist bzw- die Terroristin Computer oder Kommunikationsnetze, um genügend Zerstörung oder Störungen zu verursachen.

2. Die zehn wichtigsten Regeln für ein sicheres Verhalten im Internet".

1. Passwörter

Viele Dienste im Internet sind mit einem Zugangscode geschützt, um die Privatsphäre der Informationen zu schützen. Wenn dieses Passwort einfach oder gebräuchlich ist (sehr einfach unter Nutzern), könnte es leicht erraten werden. Aus diesem Grund wird die Verwendung von starken Passwörtern mit mehr als 8 Zeichen in Kombination mit Buchstaben (Groß- und Kleinschreibung), Ziffern und Sonderzeichen empfohlen; vermeiden Sie persönliche Informationen wie die nationale Identitätsnummer, Namen von Verwandten oder Bekannten und verwenden Sie niemals sehr einfache Muster oder Wörter aus dem Wörterbuch. Für mehr Sicherheit wird empfohlen, Passwörter periodisch zu ändern. Passwörter sollten niemals in Notizbüchern oder unverschlüsselten Dateien aufgezeichnet werden.

2. Sicherheitstechnologien

Erstellen Sie mehrere Backups aller Ihrer wichtigen Daten und stellen Sie sicher, dass sie nicht alle am gleichen Ort gespeichert sind. Halten Sie Ihre Software immer auf dem neuesten Stand. Installieren Sie einen Phishing-Filter/eine Phishing-Software in Ihrer E-Mail-Anwendung und auch in Ihrem Webbrowser.

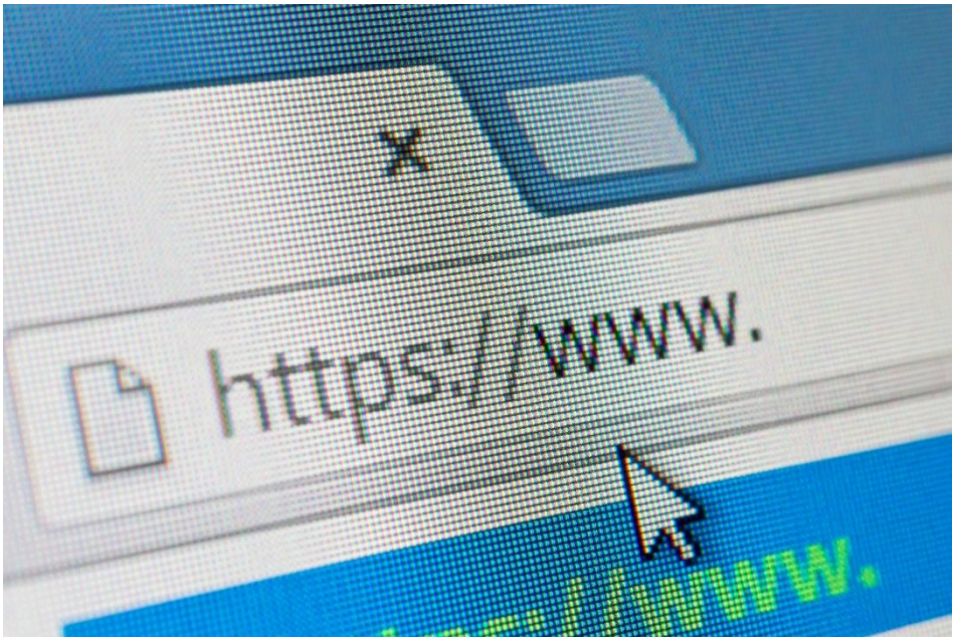
Antivirus-, Firewall- und Antispam-Lösungen sind die wichtigsten Anwendungen zum Schutz des Computers vor den wichtigsten Bedrohungen, die sich über das Internet verbreiten. Der Einsatz dieser

Technologien reduziert das Risiko und die Gefährdung durch Bedrohungen. Führen Sie zum Schutz vor Viren regelmäßig geplante Scans mit Ihrer Antiviren-Software durch und stellen Sie sicher, dass Ihre Antiviren- und Anti-Spyware-Software kompatibel sind.

3. Vertrauenswürdige Seiten

Durch Social-Engineering-Techniken werden viele Websites oft mit Daten beworben, die die Aufmerksamkeit des Nutzenden auf sich ziehen können - wie z.B. Rabatte beim Kauf von Produkten (oder sogar Gratisangebote), Scoops oder exklusives Material für aktuelle Nachrichten, Multimedia-Material usw. . Für ein sicheres Surfen wird empfohlen, dass sich der Empfänger bzw. die Empfängerin dieser Nachrichten bewusst ist und den Zugriff auf Webseiten mit diesen Merkmalen vermeidet.

Überprüfen Sie die SSL-Zugangsdaten der Website und verwenden Sie niemals persönliche/sensible Informationen auf Seiten, auf denen kein gültiges SSL-Zertifikat installiert ist.



Durch Black Hat SEO-Techniken platzieren Angreifer ihre Websites oft auf den ersten Plätzen in den Suchmaschinenergebnissen, vor allem bei der Suche nach Schlüsselwörtern, die in der Öffentlichkeit weit verbreitet sind, wie z.B. aktuelle Themen, extravagante Nachrichten oder populäre Themen (wie Sport und Sex). Bei jeder dieser Suchanfragen muss der Benutzer auf die Ergebnisse achten und überprüfen, welche Websites verlinkt werden.

Wenn wir im Internet keine Spuren hinterlassen wollen, ist einer der sichersten Wege über ein privates virtuelles Netzwerk oder über einen Proxy-Server, der als Vermittler bei der Kommunikation mit der von uns besuchten Website fungiert.

4. Informationen teilen

Alle Informationen, die wir über uns selbst ins Internet stellen, die Bilder, die wir in sozialen Netzwerken teilen, hinterlassen eine digitale Spur, die unsere so genannte "digitale Identität" ausmacht. Aus diesem Grund ist es notwendig, sich gerade bei der digitalen Identität, die wir schaffen, bewusst zu sein und nur Informationen über uns selbst hochzuladen, die wir selbst als öffentlichkeitstauglich betrachten.

Geben Sie keinen Zugang zu Ihrem Standort, Ihrer Kamera oder Ihrem Mikrofon, um zu vermeiden, dass Sie zusätzliche Informationen geben. Benutzen Sie das GPS nicht, um auf Ihren Publikationen zu zeigen, wo Sie sich befinden.

Sowohl in Instant-Messaging-Clients als auch in sozialen Netzwerken wird empfohlen, nur bekannte Kontakte zu akzeptieren und mit ihnen zu interagieren. Dadurch wird vermieden, auf die von AngreiferInnen erstellten Profile zuzugreifen, um mit den Opfern zu kommunizieren und sie verschiedenen Bedrohungen wie Malware, Phishing, Cyberbullying oder anderen auszusetzen.

5. Freie WiFi-Netzwerke

Wenn Sie ein kostenloses Wifi-Netzwerk verwenden, um öffentliche Seiten zu durchsuchen, ist das Risiko minimal. Wir müssen jedoch das Surfen auf Webseiten vermeiden, auf denen wir persönliche Daten wie Passwörter oder Benutzernamen eingeben können, da das Wifi kompromittiert werden könnte und daher jemand unsere persönlichen Daten abfangen könnte. Wir müssen die gleiche Aufmerksamkeit aufwenden, wenn wir uns mit bekannten Wifis verbinden.

6. Verdächtige Links

Eines der am weitesten verbreiteten Mittel, um Opfer auf bösartige Websites zu leiten, sind Hyperlinks oder Verweise. Wenn man diese nicht anklickt, verhindert man den Zugang zu Webseiten, die Bedrohungen enthalten, die den Nutzenden infizieren können. Links können in einer E-Mail, einem Chat-Fenster oder einer Nachricht in einem sozialen Netzwerk vorhanden sein: Der Schlüssel liegt in der Analyse, ob sie in einer verdächtigen Situation angeboten werden, die Zweifel aufkommen lässt (z.B. eine Einladung, ein Foto in einer anderen Sprache als der eigenen zu sehen), von einem unbekannten Absender stammen oder auf eine unzuverlässige Website verweisen.

7. Dateien herunterladen

Eine der größten Sicherheitsverletzungen ist das Herunterladen von Dateien. Wenn Sie sich nicht ganz sicher sind, woher das, was Sie herunterladen, stammt, vermeiden Sie es oder überprüfen Sie es vor dem Herunterladen. Viele Websites geben vor, beliebte Programme anzubieten, die verändert, modifiziert oder durch Versionen ersetzt werden, die irgendeine Art von Malware enthalten, und laden den bösartigen Code in dem Moment herunter, in dem der Nutzende ihn auf dem System installiert. Es wird daher empfohlen, beim Herunterladen von Programmen immer von den offiziellen Webseiten herunterzuladen.

Auf der anderen Seite erfolgt die Verbreitung von Malware in der Regel über ausführbare Dateien. Es wird empfohlen, das Ausführen von Dateien zu vermeiden, es sei denn, die Sicherheit der Dateien ist bekannt und ihre Herkunft ist zuverlässig (unabhängig davon, ob sie von einem Instant-Messaging-Kontakt, einer E-Mail oder einer Website stammt).

8. Aktualisieren des Betriebssystems und der Anwendungen

Das Betriebssystem (Windows, Linux, Apple ...) und alle installierten Anwendungen korrekt aktualisiert zu haben, ist eine der Hauptgarantien dafür, dass keine Türen zu Ihrem Computer offen bleiben, die von Cyberkriminellen ausgenutzt werden können. Obwohl die Aktualisierung von Computern Zeit in Anspruch nimmt und manchmal einen Neustart erfordert, ist es unerlässlich, Sicherheitslücken in der installierten Software zu beheben.

Wenn Sie beim Surfen von Ihrem Desktop- oder Laptop-PC aus bereits Vorsichtsmaßnahmen treffen, vergessen Sie Ihr Handy nicht, es ist sehr wichtig, dass Sie für diesen Fall die gleichen Regeln beachten. Durch Geräte wie Smartphones ist es wahrscheinlicher, dass die BesitzerInnen anderer Geräte Sicherheitselemente verletzen, die Ihnen Ihr Betriebssystem möglicherweise bietet.

9. Vermeiden Sie die Eingabe persönlicher Informationen in zweifelhafter Form

Wenn der Nutzende mit einem Webformular konfrontiert wird, das Felder mit sensiblen Informationen enthält (z.B. Benutzername und Passwort), wird empfohlen, die Legitimität der Site zu überprüfen. Eine gute Strategie ist es, die Domäne und die Verwendung des HTTPS-Protokolls zu überprüfen, um die Vertraulichkeit der Informationen zu gewährleisten. Auf diese Weise können Phishing-Angriffe, die

versuchen, an sensible Informationen zu gelangen, verhindert werden, indem eine vertrauenswürdige Entität simuliert wird.

10. Cookies

Ein Cookie ist eine Datei, die von einer Website erstellt wird und kleine Datenmengen enthält, die zwischen einem Sender und einem Empfänger gesendet werden, um die Präferenzen des Nutzers zu kennen. Allerdings ist es wahrscheinlich, dass die geteilten Informationen Dritte erreichen, so dass es einfach ist, den Datenverkehr dieser Daten zu beurteilen, jedenfalls können wir vom Browser aus entscheiden, diese Cookies zu löschen, um keine unnötigen Ängste zu erzeugen.

Wissen anwenden

Cyber-Kriminalität

1. Wie lautet die Definition von Cyberkriminalität?

Aufgabe: Wählen Sie die richtige Option nach dem Single-Choice-Prinzip aus: Nur eine Antwort ist richtig.

a) Cyberkriminalität beobachtet die unangemessenen Inhalte im Internet.
b) Cyberkriminalität ist eine rechtswidrige Handlung, bei der der Computer entweder ein Werkzeug oder ein Ziel oder beides ist.
c) Cyberkriminalität ist die Überwachung der Arbeits-E-Mails von Arbeitnehmern durch Arbeitgeber.
d) Cyberkriminalität ist die Beschaffung öffentlicher Informationen im Internet.

2. Welches der folgenden Beispiele ist Phishing?

Aufgabe: Wählen Sie die richtige(n) Option(en) nach dem Multiple-Choice-Prinzip aus: Es könnte mehr als eine richtige Antwort geben.

a) Sie haben eine feierliche E-Mail erhalten, dass Sie ein i-Phone gewonnen haben, und Sie sollen, um den Preis zu erhalten, einige persönliche Informationen zurücksenden.
b) Sie haben eine E-Mail mit einigen Waren erhalten, die zum Kauf angeboten wurden.

c) Sie haben eine E-Mail mit der Anforderung erhalten, das Passwort zu Ihrem Bankkonto zu ändern, mit einem direkten Link, wo Sie dies tun können.
d) Sie haben eine Informations-E-Mail über eine kulturelle Veranstaltung in Ihrer Stadt erhalten.

3. Wahr oder falsch?
Hacking kann auch als produktiver und nützlicher Akt wahrgenommen werden.
W □ F □

4. Vervollständigen Sie den Satz mit dem richtigen Wort – Wählen Sie aus der untenstehenden Auswahl ein Wort aus und füllen Sie die Lücke damit.

_____ ist der Diebstahl persönlicher Identifikationsinformationen, um illegale Handlungen zu begehen, wie z.B.: Eröffnung einer Kreditlinie, Anmietung eines Hauses, Kauf von Waren oder Dienstleistungen, Versteigerungs- und Lohnbetrug oder Erpressung.

_____ ist der ständige Kontakt mit der Person; verletzende Dinge zu der Person zu sagen oder anderen unwahren Informationen über die Person zu erzählen. Der Täter richtet zum Beispiel die Facebook-Gruppe "Ich hasse..." ein und lädt alle Freunde ein, ihr beizutreten.

_____ schließt Aktivitäten ein, die auf unehrliche Weise Reichtum für diejenigen erzeugen, die an dem fraglichen Verhalten beteiligt sind. Sie bestehen in der Ausnutzung von Insiderinformationen oder dem Erwerb von Eigentum einer anderen Person durch Täuschung, um sich einen materiellen Vorteil zu verschaffen. Unter Finanzkriminalität werden gemeinhin folgende Handlungen verstanden: Betrug, Geldwäsche, Bestechung, Bestechlichkeit und Korruption und viele andere
_____ ist eine Besessenheit davon, so viel wie möglich über die Person herauszufinden (ohne sie tatsächlich zu fragen). Zum Beispiel findet der Täter heraus, wo die Person geboren wurde, ob die Person verheiratet ist usw.

Cybermobbing, Cyberstalking, Finanzkriminalität, Identitätsdiebstahl

5. Vervollständigen Sie den Satz mit dem richtigen Wort - füllen Sie die Lücke aus.

Cyberangriff, bei dem Computer- oder Kommunikationsnetzwerke verwendet oder ausgenutzt werden, um eine ausreichende Zerstörung oder Störung zu verursachen, um Angst zu erzeugen oder eine Gesellschaft zu einem ideologischen Ziel einzuschüchtern, wird _____ genannt.

Schutz vor unangemessenen Inhalten

1. Vervollständigen Sie den Satz mit dem richtigen Wort – Wählen Sie aus der untenstehenden Auswahl ein Wort aus und füllen Sie die Lücke damit.

_____ wird als eine explizite Beschreibung oder ein Bild beschrieben, das sexuelle Gefühle stimulieren soll.
_____ ist die Förderung oder Aufstachelung zum Hass gegen Einzelpersonen oder Gruppen aus Gründen der ethnischen Herkunft, der Religion, einer Behinderung, des Alters, der Nationalität, des Veteranenstatus, der sexuellen Orientierung, des Geschlechts, der Geschlechtsidentität oder eines anderen Merkmals

_____ sind die Websites, die Anorexie als Lebensstil und nicht als Krankheit verstehen.

_____ bieten attraktive Informationen wie z.B. historische Ereignisse, aber die Fakten sind verzerrt und verweisen auf andere Informationsquellen, die bereits durch eine veränderte Wahrnehmung der Welt manipuliert wurden.

Pornographie, Pro-Ana-Webseiten, Rassismus oder Hass, Seiten mit extremistischem Inhalt

2. Welche Bewertung kann mir helfen, die Websites mit unangemessenem Inhalt zu erkennen?
Aufgabe: Wählen Sie die richtige(n) Option(en) nach dem Multiple-Choice-Prinzip aus: Es könnte mehr als eine richtige Antwort geben.

a) Anträge Bild Assoziationsbewertung (z.B. PG)
b) LT Int. Skala (z.B. LT Corporate Family Ratings)
c) Nationale Skala (z.B. NSR)
d) Online-PEGI-Bewertung (z. B. PEGI 7)

3. Welches der folgenden Werkzeuge ist die nützliche elterliche Kontrolle für Online-Inhalte?
Aufgabe: Wählen Sie die richtige Option nach dem Single-Choice-Prinzip aus: Nur eine Antwort ist richtig.

a) Online-Anwendung zum Schutz
b) iWebfilter
c) K10 Web-Schutz
d) Anti-Spiel

4. Welche Fähigkeiten sind notwendig, damit man Kinder darin unterrichten kann die Risiken der unangemessenen Inhalte zu minimieren?
Aufgabe: Wählen Sie die richtige(n) Option(en) nach dem Multiple-Choice-Prinzip aus: Es könnte mehr als eine richtige Antwort geben.

a) IT-Fähigkeiten
b) Kritisches Denken und Belastbarkeit
c) Digitale Fähigkeiten
d) Positive Wege zur Nutzung der Technik

5. Vervollständigen Sie den Satz mit dem richtigen Wort – füllen Sie Lücke aus.
Wir können hilfreiche Instrumente für den Schutz haben wie Gesetze, elterliche Kontrolle, Softwareeinstellungen, unterstützende Institutionen – aber der Schlüssel ist der/das _____ zwischen Ihnen und dem Kind.

Schutz personenbezogener Daten

1. Vervollständigen Sie den Satz mit dem richtigen Wort – Wählen Sie aus der untenstehenden Auswahl ein Wort aus und füllen Sie die Lücke damit.

_____, auch bekannt als Informationsschutz, ist ein Aspekt der Datensicherheit, der sich mit dem richtigen Umgang mit _____ befasst. Er schützt hauptsächlich die persönlichen Daten des Einzelnen vor _____. Der _____ von personenbezogenen Daten ist in Europa seit Jahren ein _____Recht. Der Datenschutz hat in den letzten Jahren aufgrund der _____ und _____, die die Erhebung, Verarbeitung, Speicherung, Verbreitung und Analyse von Daten erleichtern, immer mehr an Bedeutung gewonnen. Das _____ ist eine rechtsverbindliche Verordnung zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten.

Datenschutz, GDPR, globale Vernetzung, grundlegendes, Missbrauch, personenbezogene Daten, Schutz, technische Entwicklungen

2. Wahr oder falsch?

a) Das GDPR gilt nur für die automatische Verarbeitung personenbezogener Daten

W □ F □

b) Personenbezogene Daten beziehen sich auf sensible Daten über eine Person

W □ F □

c) Sensible Daten müssen zunehmend geschützt werden

W □ F □

d) Zu den persönlichen Daten gehören zum Beispiel Name, Geburtstag, Alter oder Wohnadresse, Kontonummer

W □ F □

e) Zu den sensiblen Daten gehören z.B. Kreditkartennummer, religiöse Überzeugung, Gewerkschaftsmitgliedschaft, Rasse und ethnische Herkunft

W □ F □

3. Vervollständigen Sie den Satz mit dem richtigen Wort – Wählen Sie aus der untenstehenden Auswahl ein Wort aus und füllen Sie die Lücke damit.

Das GDPR definiert _____ Schlüsselprinzipien, die innerhalb von _____ strikt eingehalten werden müssen. Verstöße gegen diese Grundsätze können zu _____ führen. Für _____ personenbezogene Daten verfügt das GDPR über _____ rechtmäßige Grundlagen für die Verarbeitung, da die Verarbeitung von _____ generell verboten ist, sofern nicht bestimmte Bedingungen erfüllt sind. Für die Verarbeitung von _____ gelten besondere Bedingungen. Die Datenverarbeitung ist nur in bestimmten _____ zulässig.

Ausnahmefälle, Datenverarbeitung, Höchststrafen, nicht-sensible, persönliche Daten, sechs, sensible Daten, sieben

4. Was ist bei Datenschutzverletzungen richtig?

Aufgabe: Wählen Sie die richtigen Optionen nach dem Multiple-Choice-Prinzip: Es könnte mehr als eine richtige Antwort geben.

a) Es ist die Pflicht eines für die Datenverarbeitung Verantwortlichen, den Datenverarbeiter unverzüglich über jede Datenverletzung zu informieren.
b) Bei einer Datenverletzung muss der für die Verarbeitung Verantwortliche einer Melde- und Benachrichtigungspflicht nachkommen
c) Wenn es zu einer Datenverletzung kommt, muss der Datenverarbeiter eine Melde- und Benachrichtigungspflicht erfüllen
d) Die Datenschutzbehörde muss innerhalb von 24 Stunden informiert werden.
e) Die Datenschutzbehörde muss innerhalb von 72 Stunden informiert werden.
f) Die Datenschutzbehörde muss informiert werden, wenn die Verletzung wahrscheinlich eine Gefahr für die Rechte und Freiheiten der betroffenen Personen darstellt.
g) Die zusätzliche Benachrichtigung der betroffenen Person ist nicht immer erforderlich, wenn wahrscheinlich ein hohes Risiko für die Rechte und Freiheiten der betroffenen Personen besteht.

5. Vervollständigen Sie den Satz mit dem richtigen Wort – Wählen Sie aus der untenstehenden Auswahl ein Wort aus und füllen Sie die Lücke damit.

Um den Schutz der _____ zu gewährleisten, ist die Frage der _____ ein zentrales Thema. In diesem Zusammenhang sind _____ und _____ wichtige Stichworte. _____ bezieht sich auf den Datenschutz durch _____. Das bedeutet, dass bei der Entwicklung neuer Technologien auf angemessene und datenschutzkonforme Lösungen geachtet werden muss. _____ bezieht sich auf Datenschutz durch _____. Die verantwortliche Person muss durch entsprechende Voreinstellungen sicherstellen, dass nur die _____ verarbeitet werden, die unbedingt notwendig sind.

Datensicherheit, personenbezogene Daten, personenbezogene Daten, Privacy by Default, Privacy by Default, Privacy by Design, Privacy by Design, Technologiegestaltung, , Voreinstellungen

Smartphone-Schutz

1. Welche Vorsichtsmaßnahme sollten Sie ergreifen, um Ihr Smartphone und die darauf gespeicherten privaten Daten im Falle von Verlust oder Diebstahl zu schützen?
Aufgabe: Wählen Sie die richtige(n) Option(en) nach dem Multiple-Choice-Prinzip aus: Es könnte mehr als eine richtige Antwort geben.

a) Verwenden Sie eine persönliche Identifikationsnummer und eine Bildschirmsperre
b) Verwenden Sie eine Anstecknadel mit einer gängigen Zahlenkombination, die für Sie leicht zu merken ist
c) Notieren Sie die Seriennummer Ihres Smartphones
d) Installieren Sie keine Anti-Diebstahl-Anwendung

2. Was ist in Hinsicht auf IM (Instant Messaging – Sofortnachrichten) richtig?
Aufgabe: Wählen Sie die richtige(n) Option(en) nach dem Multiple-Choice-Prinzip aus: Es könnte mehr als eine richtige Antwort geben.

a) IM (Instant Messaging) ist ein Offline-Chat zum Austausch von Nachrichten.
b) Instant Messaging ist eine internetbasierte Kommunikation über mobile Anwendungen
c) Die Nachrichtenübermittlung findet im sogenannten Pull-Verfahren statt
d) IM ist nur für die Übermittlung von Texten vorgesehen.
e) Beispiele für IM sind WhatsApp, Skype oder Facebook Messenger.

3. Die meisten IM-Anwendungen sind kostenlos. Welche Risiken sind damit verbunden?

Aufgabe: Wählen Sie die richtige(n) Option(en) nach dem Multiple-Choice-Prinzip aus: Es könnte mehr als eine richtige Antwort geben.

a) Die App muss später bezahlt werden, was mit hohen Kosten verbunden ist
b) Bei den Daten der Person handelt es sich in der Regel um das Produkt
c) Die Kommunikation ist meist verschlüsselt
d) Malware aller Art ist in den Anwendungen versteckt

4. Wahr oder falsch?

a) Es gibt kein Problem mit der uneingeschränkten App-Erlaubnis

W □ F □

b) App-Produzenten sind an Ihren persönlichen Daten interessiert

W □ F □

c) Jeder Zugriff auf persönlichen Daten ist über die Genehmigungsformulare einer App offensichtlich

W □ F □

d) Es besteht die Gefahr von Phishing

W □ F □

e) Es gibt kein Problem mit unverschlüsselter Kommunikation

W □ F □

f) Es gibt kein Problem mit unverschlüsselter Kommunikation

W □ F □

5. Vervollständigen Sie den Satz mit dem richtigen Wort – Wählen Sie aus der untenstehenden Auswahl ein Wort aus und füllen Sie die Lücke damit.

Angesichts der potenziellen _____ bei der Verwendung von Apps auf Ihrem Smartphone fragen Sie sich wahrscheinlich, wie Sie sich und Ihre Privatsphäre besser schützen können.
Hier sind einige Tipps, was Sie bei der Nutzung von Apps auf Ihrem Smartphone beachten sollten: Verwenden Sie immer die _____ Version der App, _____ Sie darauf, Bilder, die Sie nicht besitzen, als Profilbilder zu verwenden, lesen Sie vor der Installation einer App die _____ sorgfältig durch, geben Sie nur die _____ Daten ein, verwenden Sie eine _____, die nicht viel über Sie verrät und Sie nicht mit Spam belästigt, überprüfen Sie die _____ -rechte der App und passen Sie diese gegebenenfalls an, passen Sie die _____ von Apps an (z.B. Sichtbarkeit von Profilbildern) und _____ Sie unerwünschte Kontakte.

aktuellste, Blockieren, Datenschutzeinstellung, Datenschutzerklärung, notwendigsten, Sicherheitsrisiken, verzichten, Zugriffs, zusätzliche E-Mail-Adresse

Informationsstrom-/Online-Kommunikation

Co-funded by the
Erasmus+ Programme
of the European Union

1. Das gebräuchlichste Online-Kommunikationsmedium ist

Aufgabe: Wählen Sie die richtige Option nach dem Single-Choice-Prinzip aus: Nur eine Antwort ist richtig.

a) Sofortnachrichten
b) E-Mail
c) Websites

2. Vervollständigen Sie den Satz mit dem richtigen Wort – Wählen Sie aus der untenstehenden Auswahl ein Wort aus und füllen Sie die Lücke damit.

_____ sind unerwünschte E-Mails, die Sie in böser Absicht mit betrügerischen Informationen irreführen oder Sie zu schädlichen Handlungen verleiten. Bösartige Programme werden z.B. oft über _____ in gefälschten E-Mails übertragen. Es ist daher wichtig, die typischen Merkmale gefälschter E-Mails zu kennen. Achten Sie deshalb auf Folgendes: Es wird etwas versprochen, das _____ (zu gut, um wahr zu sein) scheint, der Inhalt der E-Mail passt irgendwie nicht zum (vermeintlich) vertrauenswürdigen _____, die E-Mail enthält als Betreff bestimmte _____ Wörter (z.B. letzte Erinnerung" oder "Konto gesperrt"), Sie werden gebeten, _____ anzugeben, der _____ erscheint seltsam, die E-Mail enthält viele _____ (Rechtschreibung oder Grammatik), die E-Mail wird automatisch in den _____ verschoben oder Sie werden aufgefordert, Programme mit seltsamen _____ (z.B. "jpg.vbs" oder "gif.exe") auszuführen.

Absender, Anhänge, Dateinamen, E-Mail-Absender, Fehler, Gefälschte (Fake) E-Mails, irritierende, Spam-Ordner, unrealistisch, vertrauliche Informationen

3. Foren und Chatrooms sind bekannte und beliebte Medien für Online-Kommunikation und Informationsaustausch. Welche Aussagen sind richtig?

Aufgabe: Wählen Sie die richtige(n) Option(en) nach dem Multiple-Choice-Prinzip aus: Es könnte mehr als eine richtige Antwort geben.

a) Foren eignen sich für die Kommunikation in Echtzeit
b) Chats sind für Echtzeit-Kommunikation geeignet
c) Foren eignen sich für Diskussionen, bei denen nicht alle Teilnehmer zur gleichen Zeit online sein müssen
d) Chats eignen sich für Diskussionen, bei denen nicht alle Teilnehmer zur gleichen Zeit online sein müssen
e) Foren sind besser organisiert
f) Chats sind besser organisiert
g) Nur für Foren ist eine Registrierung mit einer gültigen E-Mail-Adresse erforderlich.
h) Chats und Foren ermöglichen den Austausch von Textnachrichten, können aber in der Regel auch zum Austausch von Bildern, Videos, Links oder Dateien genutzt werden.

4. Was sind die Hauptrisiken bei der Nutzung von Foren und Chats?

Aufgabe: Wählen Sie die richtige(n) Option(en) nach dem Multiple-Choice-Prinzip aus: Es könnte mehr als eine richtige Antwort geben.

a) Falsche Identitäten
b) Malware
c) Hohe Kosten
d) Links zu Phishing-Sites
e) Unverschlüsselte Kommunikation
f) Verschlüsselte Kommunikation

5. Vervollständigen Sie den Satz mit dem richtigen Wort – Wählen Sie aus der untenstehenden Auswahl ein Wort aus und füllen Sie die Lücke damit.

In sozialen Netzwerken kann die Annahme der vermuteten Anonymität zu gedankenlosem Verhalten im Umgang mit _____ und _____ führen. Als Folge davon werden soziale Netzwerke zunehmend für _____ Aktivitäten ins Visier genommen. Es besteht die Gefahr, durch _____ oder durch die bewusste oder unbewusste Verbreitung von _____ irregeführt zu werden. Daher sollten Sie beim Umgang mit _____ immer die folgenden Aspekte berücksichtigen: Veröffentlichen und diskutieren Sie _____ und _____ Informationen niemals in einem öffentlichen virtuellen Raum, nutzen Sie die _____, um Informationen nur einem bestimmten Personenkreis zugänglich zu machen, seien Sie kritisch, wenn Sie Freunde _____, prüfen Sie bei den Einstellungen von sozialen Netzwerken den _____ und seien Sie sich der _____ Informationen bewusst. Wenn Sie Missbrauch oder Fehlverhalten in sozialen Netzwerken feststellen, sollten Sie es dem Dienstanbieter _____ und Organisationen und geeigneten _____ mitteilen.

annehmen, Behörden, betrügerische, Daten, falsche Identitäten, falschen Informationen, Filter, Informationen, melden, persönliche, Schutz der Privatsphäre, sozialen Medien, täuschenden, vertrauliche

Elterliche Kontrolle

1. Die Folgen für ein Sexting-Opfer sind

Aufgabe: Wählen Sie die richtige(n) Option(en) nach dem Multiple-Choice-Prinzip aus: Es könnte mehr als eine richtige Antwort geben.

a) Demütigung und sozialer Lynchmord für den Protagonisten der Bilder.

b) Der/Die Minderjährige wird öffentlich beleidigt, was in erster Linie sein/ihr Selbstwertgefühl beeinträchtigt, und das in einem Alter, in dem seine/ihre Persönlichkeit geformt wird und weitgehend von dem Bild abhängt, das andere verbreiten, da die Meinung der anderen wichtig ist.

c) Es gibt auch Gefühle der Hilflosigkeit, vor allem wenn der Fall den Eltern oder ErzieherInnen erzählt wird, oder Schuldgefühle, weil er/sie sich in dieser Situation befindet.

d) Es gibt keine Konsequenzen.

2. Vervollständigen Sie den Satz mit dem richtigen Wort – Wählen Sie aus der untenstehenden Auswahl ein Wort aus und füllen Sie die Lücke damit.

Grooming wird definiert als _____, das von einem _____ absichtlich durchgeführt wird, um eine Beziehung und emotionale Kontrolle über einen Minderjährigen aufzubauen, um den Weg für sexuellen _____ zu ebnen. In einigen Fällen wird es zwischen Minderjährigen durchgeführt, aber normalerweise mit einem Altersunterschied, wobei der/die Älteste in der Regel der _____ ist. Das Ziel des Grooming ist es, das Vertrauen der _____ zu gewinnen, Bilder oder Videos mit _____ Inhalt zu erhalten und sich sogar persönlich zu treffen.

Belästiger, Cybermobbing, Erwachsenen, minderjährigen Person, Missbrauch, sexuellem

3. Vervollständigen Sie den Satz mit dem richtigen Wort – Wählen Sie aus der untenstehenden Auswahl ein Wort aus und füllen Sie die Lücke damit.

Einer der ersten Schritte von _____ ist ein Mobber/eine Mobberin, welche/r das _____ beleidigt oder bedroht, indem die Person sagt, er/sie werde Informationen durchsickern lassen, die dem _____ des Opfers _____ werden. Die vom Stalker über das Opfer verbreiteten Informationen können wahr sein, aber in diesem Fall werden sie absichtlich durchgesickert, weil sie _____ oder schädlich für die Interessen des Opfers sind. Wenn verbreitete Infromationen direkt falsch bzw. unwahr sind, dann sind dies _____.

Cybermobbing, Fehlinformationen, negativ, Opfer, Ruf, schaden

4. Vervollständigen Sie den Satz mit dem richtigen Wort – Wählen Sie aus der untenstehenden Auswahl ein Wort aus und füllen Sie die Lücke damit.

Eine Möglichkeit, herauszufinden, ob ein/e _____ an _____ leidet, besteht darin, die Zeit, die mit den _____ Geräten verbracht wird, die Häufigkeit und die Auswirkungen des mangelnden Anschlusses durch Social Media zu analysieren. Wenn der/die Minderjährige _____, ängstlich oder unruhig zu sein scheint, wenn er/sie nicht mit Anderen online in Verbindung steht, oder wenn er/sie häufige _____ -schwankungen hat, könnte Netholismus der Grund dafür sein.

digitalen, emotional, Minderjährige/r, Netholismus, Stimmungs

5. Vervollständigen Sie den Satz mit dem richtigen Wort – Wählen Sie aus der untenstehenden Auswahl ein Wort aus und füllen Sie die Lücke damit.

Es können verschiedene Techniken eingesetzt werden, um _____ Daten von einem digitalen Gerät abzufangen. Manchmal verbergen die _____ ihre Absichten, indem sie als etwas anderes erscheinen, als sie sind. Zum Beispiel mittels Werbung, indem sie Informationen verlangen, um den Inhalt darstellen zu können, oder indem sie _____ verlangen, um einen _____ Dienst zu nutzen. Häufiger jedoch geben _____ ihre Daten weiter, weil sie sich der Gefahr nicht bewusst sind, so dass ein verantwortungsbewussterer Umgang mit dem _____ dringend erforderlich ist.

Internet, Minderjährige, Online, Passwörter, Täter, unbemerkt

Hardware und Software

1. Vervollständigen Sie den Satz mit dem richtigen Wort – Wählen Sie aus der untenstehenden Auswahl ein Wort aus und füllen Sie die Lücke damit.

Hardware bezieht sich auf die _____ Elemente eines Computers. Beispiele für Hardware in einem Computer sind _____. Software, allgemein als _____ bekannt, besteht aus allen Anweisungen, die der Hardware mitteilen, wie sie eine bestimmte Funktion ausführen soll. Software ist in der Lage, _____ verschiedene Aufgaben mit der gleichen grundlegenden Hardware auszuführen.

Hardware bezieht sich auf die _____ Elemente eines Computers. Beispiele für Hardware in einem Computer sind _____. Software, allgemein bekannt als _____, besteht aus allen Befehlen, die der Hardware mitteilen, wie sie eine bestimmte Funktion ausführen soll. Software ist in

der Lage, _____.verschiedene Aufgaben mit der gleichen grundlegenden Hardware auszuführen.

Monitor, Maus und Tastatur, physischen, Programme oder Anwendungen, viele

2. Welchen Tipp können Sie in Bezug auf Softwareschutz geben? (Single Choice - eine Antwort ist korrekt)

a) Regelmäßige Aktualisierungen der Software
b) Mehrere Sicherungskopien erstellen
c) Installierung keiner Software-Firewalls
d) Verschlüsselung von Informationen

3. Ein Beispiel für den Hardwareschutz ist es, den Kauf von Hardwarekomponenten aus risikoreichen Quellen/Ländern zu vermeiden (Richtig/Falsch).

a) Richtig
b) Falsch

4. Welche Maßnahmen können Sie ergreifen, um einen besseren Softwareschutz zu erreichen? (Multiple Choice - Es könnte mehr als eine richtige Antwort geben)

a) Installieren Sie ein Antivirusprogramm und halten Sie es auf dem neuesten Stand
b) Untersuchen Sie die von Ihnen installierten Sicherheitswerkzeuge
c) Ab und zu Betriebssystem-Updates installieren
d) Deaktivieren Sie die Datei- und Medienfreigabe, wenn Sie sie nicht benötigen

5. Was sind die häufigsten Angriffe auf Hardware? (Multiple Choice - Es könnte mehr als eine richtige Antwort geben)

a) Physische Unfälle
b) Modding
c) Trojaner
d) Phishing

Persönliche Daten in sozialen Medien

1. Auf welche Sicherheitsfragen sollten Sie bei der Nutzung von Social Media achten? (Multiple-Choice - Es könnte mehr als eine richtige Antwort geben)

a) Wenn ein Link Sie auf eine Website weiterleitet, sollten Sie darauf achten, ob eine physische Adresse und Kontakte vorhanden sind.
b) Sehen Sie nach, ob eine Website sowohl eine Rückgabe- als auch eine Versandpolitik hat.
c) Wenn Sie eine Freundschaftsanfrage von einer Person erhalten, die Sie nicht kennen, können Sie eine umgekehrte Bildsuche versuchen.
d) Um einen Phishing-Angriff zu vermeiden, sollten Sie die vollständige URL sehen, anhand derer Sie erkennen können, ob sie zu einer legitimen Website führt.

2. Vervollständigen Sie den Satz mit dem richtigen Wort – Wählen Sie aus der untenstehenden Auswahl ein Wort aus und füllen Sie die Lücke damit.

Die meisten Websites erlauben die Einstellung von Informationen, die als öffentliche oder private Informationen gepostet werden, durch die Verwendung der Kontrolloption "_____".

Wie persönliche Daten in einem bestimmten sozialen Netzwerk präsentiert oder gespeichert werden, liegt in der Verantwortung des _____.
Die häufigsten Angriffe in sozialen Medien verwenden eine Strategie, um den Benutzer anzulocken, nämlich durch einen _____.

Eigentümers/Anbieters sozialer Medien, Phishing-Angriff, Privatsphäre-Einstellungen

3. Welches Merkmal steht nicht im Zusammenhang mit sozialen Mediennetzwerken? (Single Choice – Eine Antwort ist korrekt)

a) Interaktiv
b) Erleichterung der Schaffung oder des Austauschs von Informationen, Ideen, Berufsinteressen und anderen Formen des Ausdrucks
c) Verbindung zwischen zwei oder mehr Personen
d) Mehr als 4 Milliarden aktive Nutzer sozialer Medien

4. Was ist kein übliches Risiko in sozialen Medien? (Single Choice – Eine Antwort ist korrekt)

a) Software, die Verschlüsselung verwendet, um den Zugang eines Zielobjekts zu seinen Daten, wie Fotos oder Dokumente, zu sperren, bis ein Lösegeld gezahlt wird
b) Art von bösartigem Code oder Software, die legitim aussieht, aber die Kontrolle über Ihren Computer übernehmen kann
c) Form von Malware, die in der Lage ist, sich selbst zu kopieren und auf andere Computer zu verbreiten
d) Form von Malware, die physischen Schaden an Ihrem Computer anrichtet.

5. Was ist keine Verteidigungsmöglichkeit gegen Cyberkriminalität in sozialen Medien? (Single Choice – Eine Antwort ist korrekt)

a) Speichern der Zugangsdaten direkt in den Geräten/Browsern/Anwendungen
b) Keine Weitergabe von persönlichen Informationen online
c) Verfügen der neuesten Sicherheitssoftware
d) Überprüfung der Datenschutzeinstellungen

Cybersicherheit

1. **Welche Aussage passt nicht zu Cybersicherheit? (Single Choice – Eine Antwort ist korrekt)**

a) Verhinderung und Aufdeckung digitaler Angriffe, Schutz von Systemen, Hardware und Software
b) Praxis der Verteidigung von Computern, Servern, mobilen Geräten, elektronischen Systemen, Netzwerken und Daten vor böswilligen Angriffen
c) Cybersicherheit gilt nur für Software und Hardware
d) Techniken zum Schutz von Computern, Netzwerken, Programmen und Daten vor unbefugtem Zugriff oder Angriffen, die auf Ausbeutung abzielen

2. Welche online Maßnahme dient nicht der Verbesserung Ihrer Cybersicherheit? (Single Choice – Eine Antwort ist korrekt)

a) Unterschiedliche Passwörter für verschiedene Konten und Profile erstellen
b) Ändern Sie Ihre Passwörter von Zeit zu Zeit und verwenden Sie eine Kombination aus Groß- und Kleinbuchstaben, Symbolen und Zahlen.
c) Speichern Sie Ihre Passwörter in einer Exceltabelle auf Ihrem Computer

d) Verwendung eines Multi-Faktor-Authentifizierungsfaktors (wenn möglich) für verschiedene Online-Konten

3. Welche der folgenden Aussagen ist keine Vorsichtsmaßnahme beim Online-Kauf? (Single Choice – Eine Antwort ist korrekt)

a) Lesen Sie Rezensionen und sehen Sie nach, ob andere Verbraucher eine positive oder negative Erfahrung mit dieser speziellen Website gemacht haben
b) Virtuelle Kreditkarten erstellen
c) Halten Sie Ihre Antiviren- und Anti-Spyware-Software zusammen mit Ihrer Firewall auf dem neuesten Stand.
d) Lesen Sie nicht die Geschäftsbedingungen der verschiedenen Websites, da sie alle sehr ähnlich sind

4. Welche der folgenden Aussagen ist bezprlich der Definition und Anwendung von Cloud Computing falsch? (Single Choice – Eine Antwort ist korrekt)

a) Praktische Anwendung eines Netzwerks von im Internet gehosteten Remote-Servern zum Speichern, Verwalten und Verarbeiten von Daten anstelle eines lokalen Servers oder eines persönlichen Computers
b) Bereitstellung verschiedener Dienste über das Internet, einschließlich Server, Speicherung, Datenbanken, Vernetzung, Software und Analytik
c) Es gibt nur eine Art von Cloud-Computing-Lösungen
d) Cloud Computing kann ohne menschliche Interaktion bereitgestellt werden

5. Welche Maßnahmen können Sie ergreifen, um Cloud Computing zu verbessern? (Multiple Choice - Es könnte mehr als eine richtige Antwort geben)

a) Verwenden Sie eine Multi-Faktor-Authentifizierung
b) Festlegung verschiedener Ebenen der Autorisierung von Informationen je nach den Bedürfnissen der Menschen
c) Gewährleistung der Ausbildung bezüglich des Schutzes von Daten und privaten Informationen
d) Sichern Sie Ihre Daten/Informationen von Zeit zu Zeit

Internet der Dinge *(IoT = Internet of Things)*

1. Welche Aussagen zu „Internet der Dinge“ sind korrekt? (Multiple Choice - Es könnte mehr als eine richtige Antwort geben)

a) Das Internet der Dinge wird den öffentlichen Verkehr verbessern
b) Das Internet der Dinge verwandelt physische Objekte in ein Ökosystem von Informationen, die zwischen tragbaren, tragbaren und sogar implantierbaren Geräten ausgetauscht werden, und macht unser Leben technologie- und datenreich.
c) Es gibt unzählige IoT-Geschäftsanwendungen
d) Intelligente Autos, tragbare Fitnessgeräte und Tracker, Sprachassistenten und intelligente Autos sind Beispiele für IoT-Technologien.

2. Welche Aussage zum Internet der Dinge ist falsch? (Single Choice – Eine Antwort ist korrekt)

a) Das IoT kann nur auf Menschen und Wohnungen sowie auf die Automobilindustrie angewandt werden

b) Internet der Dinge ist ein System von miteinander verbundenen Rechengeräten, mechanischen und digitalen Maschinen
c) Das Internet der Dinge ist eine Kombination verschiedener Technologien, Echtzeitanalyse, maschinelles Lernen, Rohstoffsensoren und eingebettete Systeme.
d) Der Begriff „Internet der Dinge“ umfasst alles, was mit dem Internet verbunden ist

3. Was sind verbreitete Anwendungen des Internet der Dinge? (Multiple Choice - Es könnte mehr als eine richtige Antwort geben)

a) Tragbares Gerät zur Blutzuckermessung
b) Ein Kühlschrank, der automatisch Einkaufslisten erstellt
c) Intelligente Städte und intelligente Wohnungen
d) Einzelhandel und verbundene Karten

4. Welche Maßnahmen können Sie anwenden, um sich vor Cyberattacken bei der Nutzung von IoT-Geräten zu schützen? (Multiple Choice - Es könnte mehr als eine richtige Antwort geben)

a) Geräte-Authentifizierung
b) Seriöse Internet-Sicherheitssoftware auf Ihren Computern, Tablets und Smartphones installieren
c) Verwendung einer VPN-Verbindung, die dazu beiträgt, die Daten, die über ein privates oder öffentliches Wi-Fi übertragen werden, zu schützen.
d) Regelmäßige Überprüfung auf Firmware-Updates auf der Website eines Geräteherstellers

5. Was sind die wichtigsten Schritte, zur Aufrechterhaltung von Cybersicherheit? (Multiple Choice - Es könnte mehr als eine richtige Antwort geben)

a) Identifizierung von Bedrohungen und Schwachstellen
b) Darstellung des Vermögensrisikos durch verschiedene Arten von Analysen
c) Entwicklung von Schutz- und Notfallplänen
d) Bestimmung des Zeitpunkts für die Alarmierung von Notfallteams, Cybersicherheitsexperten, Dienstleistungs- und/oder Versicherungsanbietern

Co-funded by the
Erasmus+ Programme
of the European Union

Lösungsschlüssel

Cyber-Kriminalität

1: b
2: a, c
3: W
4: Identitätsdiebstahl, Cybermobbing, Finanzkriminalität, Cyberstalking
5: Cyber-Terrorismus

Schutz vor unangemessenen Inhalten

1: Pornografie, Rassismus oder Hass, Pro-Ana-Webseiten, Seiten mit extremistischen Inhalten
2: a, d
3: b
4: b, d
5: Vertrauen

Schutz personenbezogener Daten

1: Datenschutz, personenbezogene Daten, Missbrauch, Schutz, grundlegendes, technische Entwicklungen, globale Vernetzung, GDPR
2: aF, bF, cW, dW, eF
3: sieben, Datenverarbeitung, Höchststrafen, nicht-sensible, sechs, persönliche Daten, sensible Daten, Ausnahmefälle
4: b, e, f
5: personenbezogene Daten, Datensicherheit, Privacy by Design, Privacy by Default, Privacy by Design, Technologiegestaltung, Privacy by Default, Voreinstellungen, personenbezogene Daten

Smartphone-Schutz

1: a, c
2: b, e
3: b, d
4: aF, bW, cF, dW, eW, fF
5: Sicherheitsrisiken, aktuellste, verzichten, Datenschutzerklärung, notwendigsten, zusätzliche E-Mail-Adresse, Zugriffs, Datenschutzeinstellung, Blockieren

Informationsstrom-/Online-Kommunikation

1b
2: Gefälschte (Fake) E-Mails, Anhänge, unrealistisch, E-Mail-Absender, irritierende, vertrauliche Informationen, Absender, Fehler, Spam-Ordner, Dateinamen
3: b, c, e, h
4: a, b, d, e
5: Daten, Informationen, betrügerische, falsche Identitäten, falschen Informationen, sozialen Medien, persönliche, vertrauliche, Filter, annehmen, Schutz der Privatsphäre, täuschenden, melden, Behörden

Elterliche Kontrolle

1: a, b, c
2: Cybermobbing, Erwachsenen, Missbrauch, Belästiger, minderjährigen Person, sexuellem
3: Cybermobbing, Opfer, Ruf, schaden, negativ, Fehlinformationen

4: Minderjährige/r, Netholismus, digitalen, emotional, Stimmungs
5: unbemerkt, Täter, Passwörter, Online, Minderjährige, Internet

Hardware und Software

1: physischen, Monitor, Maus und Tastatur, Programme oder Anwendungen, viele
2: a
3: Richtig
4: a,b,c,d
5: c, d

Persönliche Daten in Social Media

1: a, b, c, d
2: Privatsphäre-Einstellungen, Eigentümers/Anbieters sozialer Medien; Phishing-Angriff;
3: d
4: d
5: a

Cybersicherheit

1: c
2: c
3: d
4: c
5: a, b, c, d

Internet der Dinge

1: a, b, c, d
2: a
3: a, b, c, d
4: a, b, c, d
5: a, b, c, d