Risiken im Netz

VORBEUGEN, ERKENNEN UND ABWEHREN

RATGEBER

BEE SECURE

LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG
Ministère de l'Éducation nationale,
de l'Enfance et de la Jeunesse
Service national de la jeunesse

INHALTSVERZEICHNIS

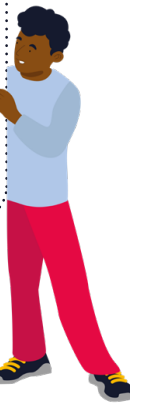
EINLEITUNG

Im Internet können Ihnen wohlmeinende Personen begegnen, Personen, die keinen wirklichen Einfluss auf Ihr Leben haben, oder auch Chancen und Gelegenheiten. Leider kann es auch Schwierigkeiten geben, Sie können Menschen mit bösen Absichten begegnen und sich vielleicht sogar Gefahren aussetzen, die Ihren Alltag beeinträchtigen können.

In dieser Publikation werden Sie verschiedene Personen kennenlernen, die in bestimmten Situationen mit Risiken im Internet konfrontiert sind. Führen Sie sie zu einem sicheren und verantwortungsbewussten Umgang mit den Informations- und Kommunikationstechnologien ! Nach jeder „Rettung" finden Sie Tipps zum Umgang mit dem jeweiligen Risiko. Diese können Sie dann in Ihren eigenen Nutzungsgewohnheiten umsetzen, um Ihre Sicherheit und Ihr Wohlbefinden, und auch möglicherweise das Ihrer Angehörigen zu verbessern.

WIE NUTZE ICH DIESEN RATGEBER ??

Nehmen Sie einen Bleistift und benutzen Sie die Klappe, um die Antworten in den Lösungsvorschlägen anzukreuzen!



1. HACKING

LYNN

28 Jahre

KONTEXT

Lynn benutzt überall fast dieselben Passwörter.

Sonst könnte sie sich die niemals alle merken!

*(**zum Beispiel:** 12345Gmail, 12345Garage, 12345TV, 1234Netflix, 12345Amazon usw.)*

Eines Abends, als sie nach Hause kommt, stellt sie fest, dass bei ihr eingebrochen wurde! Seltsamerweise wurde ihr Alarmsystem nicht ausgelöst, und es gibt keinerlei Spuren eines Einbruchs.

Bei den Ermittlungen wird festgestellt, dass die Einbrecher ihre Konten gehackt hatten, wodurch sie ganz leicht den Alarm deaktivieren und das Garagentor öffnen konnten.

Helfen Sie Lynn, angemessen zu reagieren, indem Sie aus den folgenden Handlungen auswählen:

1. alle Passwörter ändern
   (überall ein anderes sicheres Passwort)
2. nur das Passwort ihrer E-Mail-Adresse ändern
3. die Zwei-Faktor-Authentifizierung aktivieren[1]
4. ihre Kreditkarten sperren[2]
5. sich erkundigen, welche Informationen über sie im Netz zirkulieren, und die Löschung privater Inhalte verlangen

TIPPS

VERWENDEN SIE EINEN PASSWORT-MANAGER.

Dadurch können Sie

- alle Ihre Passwörter an einem Ort aufbewahren,
- sichere Passwörter erzeugen, die Sie sich nicht merken müssen,
- aus zwei Möglichkeiten für die Speicherung Ihrer Daten wählen:
  - **Online-Manager**[3]**:** die Daten werden auf einem internen Server oder in einer Cloud gespeichert[4]
  - **Offline-Manager**[5]**:** die Daten werden auf dem Computer des Nutzers gespeichert.

Wählen Sie ein sicheres und einzigartiges Passwort für Ihren Manager und teilen Sie es mit niemandem. Aktivieren Sie die Zwei-Faktor-Authentifizierung!

ERSTELLEN SIE IN 2 SCHRITTEN EIN SICHERES PASSWORT:

- Wählen Sie einen Satz, den Sie sich leicht merken können, der keine persönlichen Informationen enthält.
- Verwenden Sie mindestens 12 Zeichen.

(**Beispiel:** 2dinosaurierlebenaufdemmars)

Testen Sie die Sicherheit Ihres Passworts:
https://pwdtest.bee-secure.lu

Prüfen Sie, ob Ihr Konto gehackt wurde:
https://haveibeenpwned.com

[1] Authentifizierungsmethode, bei der ein Nutzer gezwungen wird, zwei verschiedene Identitätsnachweise zu liefern (zum Beispiel Passwort plus „Token" oder Fingerabdruck). I [2] Im Großherzogtum Luxemburg: rufen Sie sofort unter (+352) 49 10 10 an (24/7 erreichbar), um Ihre Kreditkarten zu sperren, und informieren Sie Ihre Bank. I [3] Zum Beispiel: LastPass, Sticky Password I [4] Weitere Informationen zum Thema Cloud, S. 11 I [5] Zum Beispiel: KeePassX

2. EINSTELLUNGEN UND WOHLBEFINDEN

LARA
14 Jahre

KONTEXT

Lara möchte negative Auswirkungen von Bildschirmzeit auf ihr Wohlbefinden bestmöglich vermeiden. Dazu hat sie beschlossen:

- Bildschirme während der Mahlzeiten zu vermeiden
- Benachrichtigungen auf ihrem Smartphone zu deaktivieren
- das WLAN von 21:30 bis 07:00 Uhr auszuschalten
- die Funktion „*automatische Wiedergabe*“ auf Video-Plattformen zu deaktivieren[6]

Die Bildschirmzeit insgesamt zu reduzieren, ist schon ein guter Anfang, aber man muss auch die

_ _ C _ _ _ _ _ _ E
S _ _ _ _ _ _ _ _ T
BERÜCKSICHTIGEN!

TIPPS

ES IST AUCH SEHR WICHTIG, DIE GERÄTE MIT HILFE DER RICHTIGEN EINSTELLUNGEN ZU SICHERN:

- gesperrte Nutzerkonten[7] für alle Dienste und Geräte
- Pop-up-Werbung blockieren und integrierte („*In-App*“-) Käufe deaktivieren
- automatische Updates aktivieren
- automatische Sperre bei Inaktivität aktivieren
- unnötige Berechtigungen deaktivieren, um das Teilen von Daten zu begrenzen

(persönliche Informationen, Geolokalisierungsdaten, Audio-/Video-Aufnahmen, Spracherkennung)

- sich bestmöglich vor Viren und Gefahren schützen:
  - Installieren Sie auf Ihren Computern, Laptops und Macs ein Antivirenprogramm.
  - Stellen Sie sicher, dass Ihr Antivirenprogramm regelmäßige Updates erhält.
  - Führen Sie regelmäßig manuelle Scans für Ihre gesamte Festplatte durch.

SCHÜTZEN SIE IHRE IM WLAN ÜBERTRAGENEN DATEN

Nutzen Sie dazu:

- ein sicheres Passwort für die Anmeldung im Netzwerk
- WPA3 als Verschlüsselungsmodus für Ihren Router (das neueste und sicherste derzeit verfügbare Protokoll)

Wenn Ihr Gerät WPA3 nicht unterstützt, nutzen Sie WPA2.

[6] YouTube, Disney+, Netflix usw. I [7] Durch Passwörter, Codes, Gesichtserkennung und/oder Fingerabdrücke geschützte Konten

3. PHISHING-ATTACKE

DENNIS
25 JAHRE

KONTEXT

Dennis ist Opfer einer Phishing-Attacke.

Helfen Sie Dennis, die Risiken zu erkennen:

1. Der Link führt auf eine gefälschte Webseite, die zur Eingabe von persönlichen Informationen auffordert.[8]
2. Der Link führt auf eine authentische Webseite und fordert zur Eingabe persönlicher Informationen auf.

TIPPS

BEVOR SIE AUF EINE E-MAIL REAGIEREN, DEREN ABSENDER SIE NICHT SOFORT ERKENNEN, SOLLTEN SIE KRITISCH SEIN:

1. Haben Sie ein Konto bei diesem Anbieter?
2. Der Absender
   - Kennen Sie ihn?
   - Entspricht die E-Mail-Adresse der Adresse des Absenders?
   - Handelt es sich um die offizielle E-Mail-Adresse?
3. Führt Sie der Link zur offiziellen Webseite des Anbieters?

Wenn Sie eine oder mehrere dieser Fragen verneint haben, seien Sie vorsichtig:

- Kontaktieren Sie sofort den **offiziellen Service des betreffenden Anbieters**, um sich zu informieren (in Alex' Fall wäre das der **Helpdesk** seiner Bank).
- Melden Sie die E-Mail beim **CIRCL**[9] (**C**omputer **I**ncident **R**esponse **C**enter **L**uxembourg) oder über **SPAMBEE**[10] , einem kostenlosen Plug-in für Ihren Internetbrowser.
- Öffnen Sie den Anhang nicht, er könnte **Malware enthalten**.

Malware, die ganz diskret personenbezogene Daten ausspionieren soll, wird nicht per E-Mail angekündigt, und Sicherheitspatches werden NIEMALS per E-Mail verschickt!

Wenn Sie Opfer von Phishing werden, reagieren Sie schnellstmöglich auf diese Datenschutzverletzung![11]

[8] Passwörter, Kontonummern, Kreditkarten usw. I [9] https://circl.lu/report/#report-an-incident I [10] www.spambee.lu I [11] Siehe Frage unter „Hacking", S. 4.

4. SPEICHERMEDIEN

JULIE
14 Jahre

CONTEXTE

Julie schreibt gerade die Abschlussarbeit für ihr Studium. Im Moment sind ihre Dateien lokal auf ihrem PC gespeichert, aber wie alle Speichermedien ist er nicht zu 100 % sicher!

Helfen Sie Julie, ihr Speichersystem zu diversifizieren:

1. USB-Stick
2. Papierausdruck
3. Cloud
4. externe Festplatte

TIPPS

Die Cloud lässt Sie überall, von jedem Gerät oder Terminal aus, auf Ihre Dokumente, Fotos oder andere Dateien zugreifen. Das macht Ihnen das Leben leichter, aber achten Sie darauf, Ihre Daten zu schützen:

- verwenden Sie ein sicheres Passwort und wenn möglich Zwei-Faktor-Authentifizierung
- schützen Sie alle Geräte, die damit verbunden sind[12]
- verschlüsseln[13] Sie sensible Dokumente oder Daten, die in der Cloud gespeichert werden (zum Beispiel: VeraCrypt[14], Cryptomator[15])

Lesen Sie die Nutzungsbedingungen und Garantien der verschiedenen Dienste aufmerksam durch:

- Wer hat Zugriff auf Ihre Daten?
- Wie kann der Cloud-Anbieter sie nutzen?
- Welche Garantien werden bezüglich des Datenschutzes gegeben?
- Was passiert im Falle einer Unterbrechung oder Einstellung des Service?
- Wird die Zerstörung Ihrer Daten gewährleistet, wenn Sie sie löschen?

GENERELL:

- Wenn Sie sich über das Gerät eines Dritten mit einem Konto verbinden, nutzen Sie den „Inkognito"-Modus[16] (personenbezogene Daten / Passwörter werden nicht gespeichert).
- Vermeiden Sie unbekannte USB-Sticks, die Malware enthalten könnten.
- Was Unterhaltungsmedien (Literatur, Kunst, Musik, Film, Videospiele usw.) angeht, prüfen Sie, ob diese urheberrechtlich geschützt sind.
  - Laden Sie Ihre Video- und Audioinhalte nur von legalen Webseiten herunter.
  - Zitieren Sie alle Quellen, die Sie beim Verfassen einer Arbeit genutzt haben.

Gesetze gelten auch im Internet.
Unwissenheit schützt nicht vor Strafe!

[12] Siehe S. 5 unter „Einstellungen und Wohlbefinden" | [13] Die Daten werden in einer Form codiert, sodass man sie ohne den passenden Schlüssel nicht lesen kann. | [14] www.veracrypt.fr/en/Home.html | [15] https://github.com/cryptomator/cryptomator | [16] STRG-UMSCHALT-P in Firefox oder Internet Explorer, STRG-UMSCHALT-N in Chrome

LISA
25 JAHRE

5. VERBREITUNG VON INFORMATIONEN

KONTEXT

Lisa ist mit einem Freund auf Safari in Südafrika und teilt ein Selfie mit einem Nashorn auf Social Media.

Welche Informationen könnten Dritte aus diesem Foto herauslesen?

1. Ort
2. geografische Koordinaten
3. Uhrzeit
4. Ferienart
5. Namen
6. Vornamen
7. Kameramodell
8. Ausrichtung der Kamera
9. Brennweite
10. Belichtung
11. Lichtstärke
12. Blitz
13. ISO-Wert

All diese Daten zu teilen, ist nicht ohne Risiko. Was sind potenzielle Gefahren?

1. Überwachung
2. Gefährdung des Nashorns
3. Verlust der informativen Selbstbestimmung
4. Datenverkauf

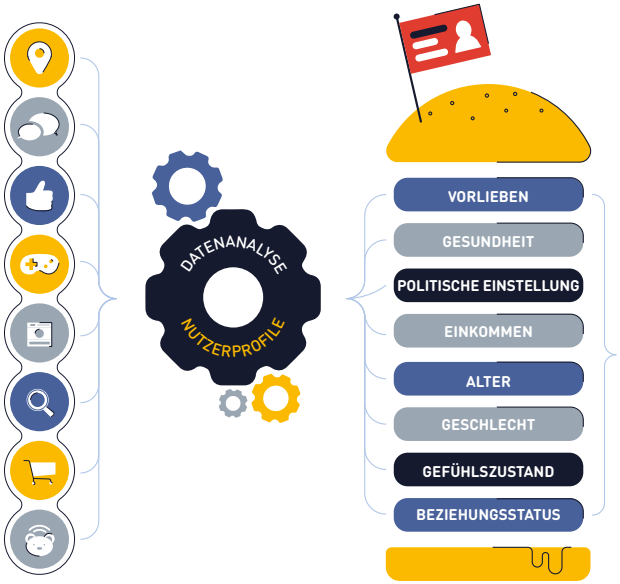
TIPPS 1/2

SCHRÄNKEN SIE DIE WEITERGABE IHRER DATEN EIN.

Jede Handlung im Internet (Klick, Like, Post, Diskussion, Suche, Einkauf, Anmeldung usw.) hinterlässt eine digitale Spur in Form von Daten.

Ohne Beschränkung der Weitergabe können anhand dieser Informationen

- Menschen mit bösen Absichten Ihre Aktivitäten sowie Ihren Standort verfolgen
- Firmen virtuelle Profile erstellen und diese Daten selbst verarbeiten oder an Dritte verkaufen



ENTSCHEIDUNGEN ÜBER

- die angezeigten Inhalte
- die angezeigte Werbung
- die angezeigte Produktliste
- Ihre Behandlung als Kunde
- Ihre Kreditwürdigkeit
- esw.

TIPPS 2/2

WIE SCHRÄNKT MAN DIE WEITERGABE VON DATEN EIN?

- Lesen Sie die Nutzungsbedingungen und Garantien der verschiedenen Dienste aufmerksam durch[17].
- Deaktivieren Sie unnötige Berechtigungen[18].
- Die Kunst, weniger über sich zu sagen: Es müssen nicht alle alles wissen.
- Nutzen Sie eine Haupt-E-Mail-Adresse für vertrauliche und eine zweite E-Mail-Adresse (oder ein Pseudonym) für öffentliche Kontakte.
- Passen Sie die Privatsphäre-Einstellungen an und überprüfen Sie sie erneut bei Änderungen der Plattform/seitens des Anbieters.
- Löschen Sie Konten, die Sie nicht mehr nutzen.
- Lehnen Sie nicht erforderliche Cookies ab.
- Nutzen Sie datensparende Tools (zum Beispiel: Privacy Badger, Startpage).
- Löschen Sie die Metadaten eines Fotos / Videos, bevor Sie es posten[19].

DIE DATENSCHUTZGRUNDVERORDNUNG DER EUROPÄISCHEN UNION (DSGVO)

- schützt die personenbezogenen Daten der Internetnutzer (alle Informationen, mit denen man eine Person identifizieren kann oder die sie identifizierbar machen);
- sieht eine Reihe von Verpflichtungen und Rechten für Unternehmen und Nutzer vor, um Transparenz bei Aufbewahrung, Übertragung und Nutzung der Daten zu gewährleisten[20].

Wenn Ihre Rechte nicht respektiert werden:

- Kontaktieren Sie den Verantwortlichen für die Verarbeitung („*DPO*“).
- Wenn Ihr Vorgehen folgenlos bleibt:
  - ◊ Legen Sie Beschwerde bei der CNPD[21] ein.
  - ◊ Wenden Sie sich an einen Anwalt und reichen Sie Klage ein[22].

[17] Siehe S. 11: Fragen, die man sich stellen sollte, bevor man sich bei einem Dienst anmeldet. I [18] Persönliche Informationen, Geolokalisierung, Audio-/Videoaufnahmen, Spracherkennung I [19] www.makeuseof.com/tag/3-ways-to-remove-exif-metadata-from-photos-and-why-you-might-want-to I [20] Für weitere Informationen siehe www.bee-secure.lu/dsgvo I [21] https://cnpd.public.lu/fr/particuliers/faire-valoir/formulaire-plainte.html I [22] Stellen Sie vorher sicher, dass Sie alle anderen Maßnahmen ergriffen haben. Ein Prozess kann teuer und langwierig werden.

6. BETRUG

SASHA

16 JAHRE

KONTEXT

Sasha möchte sich ein Videospiel für seine neue Konsole kaufen. Er hat auf den Black Friday gewartet und hofft auf ein Schnäppchen.

Helfen Sie Sasha dabei, zu verstehen, dass es sich um Abzocke handelt! Was sind die sichtbaren Indikatoren auf der Webseite?

TIPPS

PRÜFEN SIE DIE VERTRAUENSWÜRDIGKEIT DER WEBSEITE.

- Ist der Kaufpreis realistisch?
- Hat die Webseite ein Impressum?
- Sind die Vertragsbedingungen transparent?
- Werden die übermittelten Daten beim Kauf verschlüsselt (HTTPS)?
- Wie bewerten andere Käufer den Händler?
- Bietet die Webseite sichere Zahlungsmethoden an (Rechnung, bei Lieferung, elektronisches Zahlungssystem)?
- Gibt es Kontaktmöglichkeiten zum Händler?

NUTZEN SIE BEI JEDER TRANSAKTION IM NETZ:

- eine Zwei-Faktor-Authentifizierung[23]
- ein sicheres Passwort
- eine private WLAN-Verbindung (kein öffentliches Netzwerk)
- eine gesicherte HTTPS-Verbindung

HTTPS, ein sicheres Übertragungsprotokoll: mit diesem Protokoll wird der Austausch von Daten zwischen dem Nutzer einer Webseite und dem Server, der die Webseite beherbergt, verschlüsselt. Dadurch lässt sich vermeiden, dass Ihre Daten von Dritten abgefangen oder gelesen werden.[24]

Installieren Sie das Plug-in HTTPS everywhere in Ihrem Internetbrowser!

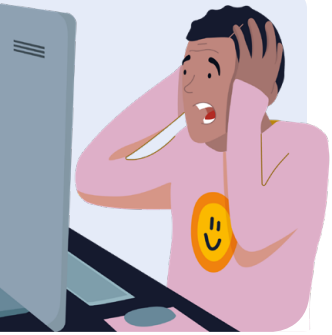
Hüten Sie sich vor (öffentlichen) WLAN-Verbindungen ohne Passwort: Jede Kommunikation kann für andere verbundene Geräte sichtbar sein, was den Diebstahl von Passwörtern, Benutzernamen und/oder anderen Daten ermöglicht.

[23] Siehe Seite 4 I [24] Ein SSL-/TLS-Zertifikat zusätzlich zum HTTPS ist wichtig für Webseiten, auf denen Sie personenbezogene Daten wie Bankdaten oder Kreditkartendaten eingeben. Zur Überprüfung können Sie auf das „Vorhängeschloss" in der Adressleiste klicken.

7. DESINFORMATION

PIERRE

13 Jahre



KONTEXT

Pierre entdeckt einen Post:

Nach einiger Suche findet er heraus, dass das Foto von einer Satire-Webseite[25] stammt, die ihren Nutzern ganz klar mitteilt, dass keiner ihrer Beiträge echt ist. Der Urheber des Social-Media-Posts hat wissentlich eine satirische Information verbreitet, ohne das zu erwähnen. Somit wird sie zur **Desinformation**.

Helfen Sie Pierre dabei, die Risiken der Desinformation zu verstehen:

1. Desinformation kann echte gesellschaftliche und politische Folgen haben.
2. Desinformation macht Internetnutzer immer dümmer.

TIPPS

VERMEIDEN SIE ES, DESINFORMATION, FAKE NEWS ODER HOAXES WEITERZUVERBREITEN!

- Hinterfragen Sie die Information:
  - Wer verbirgt sich dahinter?
  - Ist die Quelle vertrauenswürdig?
  - Wie berichten andere über das Thema?
- Informieren Sie Ihre Kontakte, wenn sie Desinformationen verbreiten.
- Melden Sie Desinformationen auf der Plattform.
- E-Mails und Nachrichten, die Sie dazu auffordern, sie mit all Ihren Kontakte zu teilen (Kettenbriefe), sind fast immer ein Hoax oder Abzocke.

Prüfen Sie die erhaltenen Informationen im Zweifelsfall über Seiten wie zum Beispiel www.hoaxbuster.com oder www.mimikama.at.

[25] Quelle: Der Postillon. Erstes Baby mit Maske geboren, 2020. Screenshot: www.der-postillon.com/2020/09/baby-maske.html

8. ILLEGALE INHALTE

PIT

35 Jahre

KONTEXT

Pit scrollt durch seinen Newsfeed auf einer Social-Media-Plattform und beteiligt sich an der Veröffentlichung von Hasskommentaren in Verbindung mit Asylbewerbern und Geflüchteten, die mit dem Lkw nach Großbritannien gelangen:

Zozo_78

Eine gute Kalaschnikow mit genug Munition wirkt Wunder. Eine schlechte Kalaschnikow wäre noch besser, weil sie weiter streut!!! 😜

Gefällt mir · Kommentieren · Teilen 18:52

Sonix-2002

Napalm kostet nicht mal die Hälfte! ;)

Gefällt mir · Kommentieren · Teilen 19:05

Smileyface

Man sollte Abgase in den Anhänger lassen. 💨

Gefällt mir · Kommentieren · Teilen 19:12

Ist ein solches Verhalten im Internet strafbar?

1. Ja
2. Nein

TIPPS

HINTER JEDEM BILDSCHIRM VERBIRGT SICH EIN MENSCH, DESWEGEN IST ES WICHTIG:

- höflich und respektvoll zu bleiben
- andere Meinungen und Ansichten zu respektieren
- niemals etwas mit Wut im Bauch zu schreiben
- niemals zu Gewalt aufzurufen

TRAGEN SIE ZUM KAMPF GEGEN ILLEGALE INHALTE BEI, MELDEN SIE SIE BEI DER JEWEILIGEN PLATTFORM UND ANONYM UNTER:

BEE SECURE STOPLINE ILLEGALE INHALTE MELDEN stopline.bee-secure.lu

Das betrifft:

- rassistische, revisionistische und diskriminierende Inhalte (einschließlich Hatespeech)
- Darstellung von sexuellem Missbrauch an Minderjährigen
- terroristische Inhalte

Um das Zusammenleben im Internet noch angenehmer zu gestalten, die meisten Communities und Webseiten einen Verhaltenskodex zur Verfügung. Bitte respektieren Sie die Grundsätze der „***Netiquette***“[26] !

[26] www.bee-secure.lu/netiquette

9. SEXTING

PASCAL
16 Jahre
SAM 18 Jahre

KONTEXT

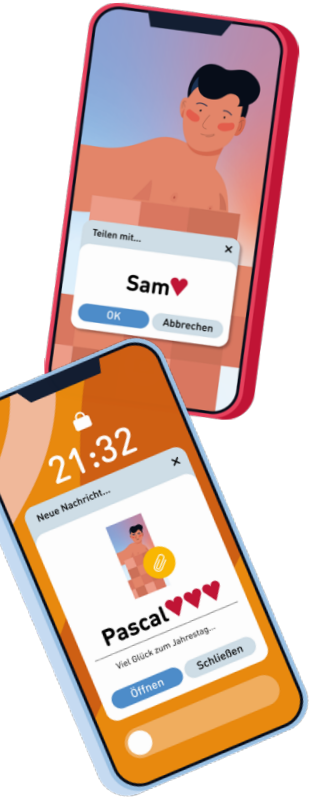
Pascal überlegt, ob er Sam zu ihrem Jahrestag ein intimes Selfie schicken soll. Er wägt **Pro** und **Contra** ab:

PRO

- Er vertraut Sam und denkt nicht, dass Sam das Foto mit anderen teilen würde.
- Falls das Foto gespeichert wird, würde Sam es löschen, wenn Pascal darum bittet.
- Es ist aufregend, ein intimes Foto zu verschicken.

CONTRA

- Wenn Sams Daten nicht gut gesichert sind[27], könnte das Foto gegen beider Willen geteilt werden.
- Wenn sie sich irgendwann im Schlechten trennen, könnte Sam beschließen, das Foto mit anderen oder auf einer Webseite zu teilen.



Pascal hat noch nicht alle nötigen Informationen, um eine aufgeklärte Entscheidung zu treffen. Darf Pascal aus rechtlicher Sicht ein intimes Foto von sich selbst teilen?

1. **Ja**, nur Sam begeht eine Straftat beim Teilen von Pascals Foto ohne sein Einverständnis.
2. **Nein**, Pascal ist noch nicht 18 und begeht daher eine Straftat, wenn er ein intimes Foto von sich selbst erzeugt, besitzt und teilt.
3. **Ja**, Pascal ist 16 und begeht daher keine Straftat, wenn er ein intimes Foto von sich selbst erzeugt, besitzt und teilt.
4. **Ja**, Pascal kann mit seinem Foto machen, was er will.

TIPPS

INTIME INHALTE[28] VON IHNEN ZIRKULIEREN IM NETZ?

Manchmal reicht es, sofort freundlich, aber bestimmt die Person darüber zu informieren, dass sie Ihr Recht am eigenen Bild verletzt und die Inhalte löschen muss. Wenn sie sich weigert und/oder als Erpressung weitere Inhalte fordert:

- Reagieren Sie nicht mehr auf ihre Nachrichten.
- Sammeln Sie Beweise.
- Erstatten Sie schnellstmöglich Anzeige bei der Polizei.

Wenn Sie minderjährig sind und Ihr intimes Foto geteilt haben, lassen Sie sich nicht davon abschrecken, dass Sie eine Straftat begangen haben. Sie werden über die Fakten aufgeklärt, und die Polizei wird alles in ihrer Macht Stehende tun, um Ihnen zu helfen.

- Nutzen Sie die Funktionen „*melden*“ und „*blockieren*“ auf der Social-Media-Plattform.
- Bleiben Sie nicht allein.

Kostenlose, anonyme und vertrauenswürdige **telefonische und Online-Beratungsstellen** sind auch eine gute Anlaufstelle, um angemessene Hilfe zu finden:

BEE SECURE HELPLINE BERATUNG Tel: 8002 1234

kanner jugend telefon 116111

Online Help (www.kjt.lu)

Schriftliche Online-Beratung für Kinder und Jugendliche

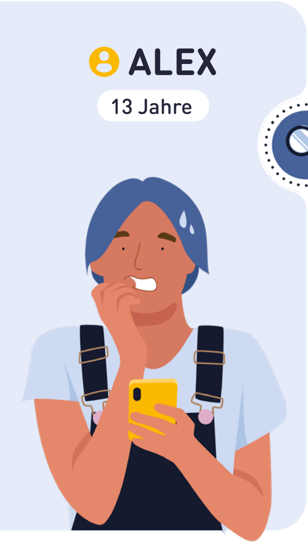
Chatberodung (www.kjt.lu)

Beratung per Live-Chat für Kinder und Jugendliche

Für weitere Informationen zum gesetzlichen Rahmen, zur Erstattung einer Anzeige und wie man bei Konfrontationen reagieren sollte: **www.bee-secure.lu/sexting-ratgeber**.

[27] Schwache Passwörter, keine regelmäßigen Updates, keine Zwei-Faktor-Authentifizierung usw. I [28] Video oder Foto

10. CYBER-MOBBING



KONTEXT

In einem Chat wurde Denis nach einem peinlichen Foto von ihm, das auf Social Media geteilt wurde, von seinen Mitschülern beleidigt und er erhielt unangenehme Nachrichten.

Denis weiß nicht, was er tun soll. Was raten Sie ihm?

1. „Bitte die Person, die das Foto geteilt hat, es zu löschen.“
2. „Tu so, als wär nichts, morgen lachen sie schon wieder über jemand anderen.“

TIPPS

Aktivieren Sie auf der betreffenden Social Media-Plattform die Funktion, mit der Tags in Posts manuell bestätigt werden müssen.

Bitten Sie die Personen auf den Fotos um Erlaubnis , bevor Sie sie posten. In Luxemburg gelten die Gesetze zum Recht am eigenen Bild wie in anderen Ländern auch!

Das Recht am eigenen Bild ist nicht vergänglich. Man hat jederzeit das Recht, die Löschung eines Inhaltes zu verlangen!

SIND SIE OPFER VON CYBER-MOBBING?

- Antworten Sie nicht auf Nachrichten.
- Sammeln Sie Beweise (Sie können Anzeige erstatten!).
- Nutzen Sie die Funktionen „*melden*“ und „*blockieren*“ auf der Social-Media-Plattform.
- Bleiben Sie nicht allein.

Kostenlose, anonyme und vertrauenswürdige **telefonische und Online-Beratungsstellen** sind auch eine gute Anlaufstelle, um angemessene Hilfe zu finden:

BEE SECURE HELPLINE BERATUNG Tel: 8002 1234

kanner jugendtelefon 116111

Online Help (www.kjt.lu)

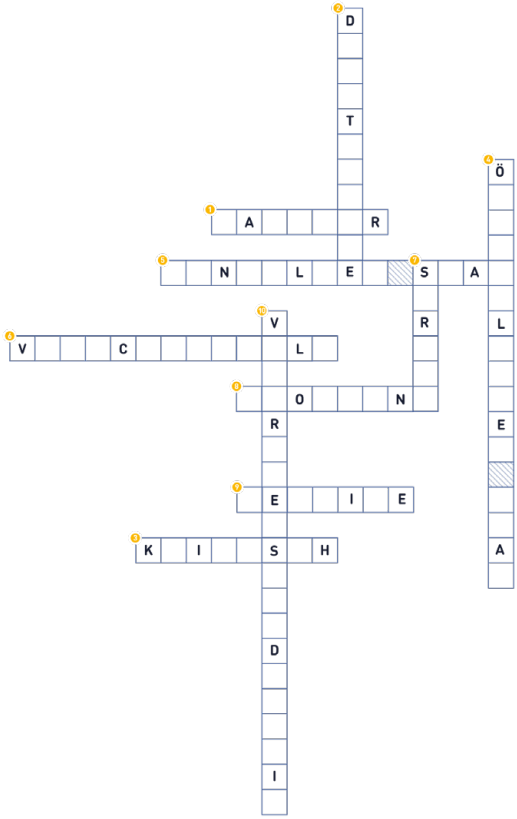
Schriftliche Online-Beratung für Kinder und Jugendliche

Chatberodung (www.kjt.lu)

Beratung per Live-Chat für Kinder und Jugendliche

Für weitere Informationen zum gesetzlichen Rahmen, zur Erstattung einer Anzeige und wie man bei Konfrontationen reagieren sollte: **www.bee-secure.lu/cyber-mobbing-ratgeber**.

KREUZWORTRÄTSEL: WAS HABEN SIE BEHALTEN?



1 Ich nutze einen ....., um meine Passwörter sicher an einem Ort zu speichern.

2 Ich ..... alle unnötigen Berechtigungen, um meine Daten zu schützen.

3 Ich bleibe ..... gegenüber unbekannten E-Mails und Informationen im Netz.

4 Ich vermeide Online-Transaktionen im .....

5 Auch wenn ich automatische Updates aktiviere und ein Antivirenprogramm habe, führe ich regelmäßig einen ..... auf meiner Festplatte durch.

6 Ich ..... sensible Dokumente oder Daten, die in der Cloud gespeichert werden.

7 Unwissenheit schützt nicht vor .....

8 Ich trage zum Kampf gegen illegale Inhalte bei, indem ich sie bei der BEE SECURE ..... melde.

9 Wenn ich Opfer einer ungewollten Veröffentlichung intimer Inhalte werde, sammle ich ....., um Anzeige zu erstatten.

10 Ich prüfe die ..... einer Webseite, bevor ich dort ein Produkt kaufe oder einen Service bestelle.

ANLAUFSTELLEN

HILFE UND BERATUNG

BEE SECURE Helpline

Kostenlose telefonische Beratungsstelle. Alle Bürger egal welchen Alters können dort Fragen zur sicheren, verantwortungsbewussten und positiven Nutzung von Informations- und Kommunikationstechnologien (IKT) stellen, zum Beispiel im Kontext von Cyber-Mobbing, Social Media, Recht auf Privatsphäre, technische Sicherheit und mehr.

Die BEE SECURE Helpline ist die erste Anlaufstelle für diese Fragen und bietet eine anonyme und vertrauensvolle Beratung an.

BEE SECURE HELPLINE BERATUNG
Tel: 8002 1234

KJT

Das KJT berät und unterstützt Kinder und Jugendliche sowie ihre Bezugspersonen bei ihren alltäglichen Sorgen und Fragen, Ängsten, Problemen und Krisen.

„Niemand soll alleine bleiben."

Jedes Kind und jeder Jugendliche kann sich direkt an speziell ausgebildete Berater wenden. Eltern und andere Bezugspersonen der Kinder sowie pädagogische und psychologische Fachkräfte haben ebenfalls die Möglichkeit das niederschwellige Beratungsangebot zu nutzen.

KJT

- Kanner-Jugendtelefon **116 111**
- Online Help *(**www.kjt.lu**)*
- Chatberodung *(**www.kjt.lu**)*
- Elterntelefon **26 64 05 55**

Anonym Glécksspiller a.s.b.l.

Die Beratungsstelle „Game Over“ von Anonym Glécksspiller ist der Ansprechpartner für alle Fragen rund um die gesunde Nutzung von digitalen Medien. Neben der Bildung und Information von Eltern und Jugendlichen umfasst der Service eine Diagnostik bei Verdachtsfällen der exzessiven Internetnutzung, erzieherische Tipps für Familien zum Thema Medien sowie die Möglichkeit einer psychotherapeutischen Unterstützung.

https://gameover.lu

Union luxembourgeoise des consommateurs (ULC)

Die ULC ist eine Vereinigung ohne Gewinnzweck, welche den Schutz, die Verteidigung, die Information sowie die Bildung der Luxemburger Verbraucher zum Ziel hat. Als national repräsentative Organisation vertritt sie die Verbraucher auch bei den öffentlichen und politischen Instanzen.

www.ulc.lu

MELDUNGEN UND BESCHWERDEN

BEE SECURE Stopline

Tragen Sie zum Kampf gegen illegale Inhalte bei, indem Sie sie anonym unter https://stopline.bee-secure.lu melden. Das betrifft die Darstellung von sexuellem Missbrauch an Minderjährigen, rassistische, revisionistische und diskriminierende Inhalte (einschließlich Hatespeech) und terroristische Inhalte.

Institut Luxembourgeois de Régulation (ILR)

Das ILR überwacht den Elektrizitätsmarkt und die dort tätigen Akteure. Man unterscheidet insbesondere zwischen Erzeugern, Anbietern und Netzbetreibern.

Sie können sich in folgenden Fällen an das ILR wenden:

- bei Schwierigkeiten, ein Problem mit einem Anbieter oder einem Netzbetreiber zu lösen, für eine Schlichtung oder in bestimmten Fällen für ein Beilegungsverfahren von Streitigkeiten
- für alle Fragen über den Elektrizitätsmarkt (zentrale Anlaufstelle)

https://web.ilr.lu

Europäisches Verbraucherzentrum Luxemburg (EVZ Luxemburg)

Das EVZ Luxemburg ist Teil eines Netzwerks aus 29 Europäischen Verbraucherzentren in der Europäischen Union sowie in Island und Norwegen (European Consumer Centre Network – ECC-Net).

Das ECC-Net erfüllt vor allem die folgenden Aufgaben:

- Information für Verbraucher über europäisches Verbraucherrecht und europäische Verbraucherrechtspolitik
- Beratung von Verbrauchern in grenzüberschreitenden Verbraucherrechtsstreitigkeiten
- Unterstützung der Verbraucher in grenzüberschreitenden Verbraucherrechtsstreitigkeiten mit einem Unternehmen in einem anderen Land der EU, in Island oder in Norwegen

www.cecluxembourg.lu

Computer Incident Response Center Luxembourg (CIRCL)

Das CIRCL ist eine Regierungsinitiative, die Gefahren und Vorfälle der IT-Sicherheit erheben, prüfen, melden und darauf reagieren soll.

Melden Sie Phishing-Attacken:

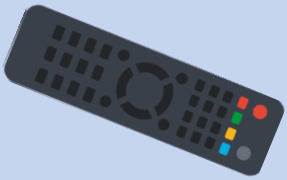
https://circl.lu/report/#report-an-incident

Nationale Kommission für den Datenschutz (Commission nationale pour la Protection des Données, CNPD)

Öffentliche Einrichtung zur Prüfung der Legalität von Dateien und allen Erhebungen, Nutzungen und Übertragungen von Informationen, die identifizierbare Einzelpersonen betreffen, und zur Sicherstellung der Einhaltung der Freiheiten und Grundrechte physischer Personen und insbesondere ihres Privatlebens.

Wenn Sie eine Beschwerde einreichen möchten:

https://cnpd.public.lu/fr/particuliers/faire-valoir/formulaire-plainte.html



LÖSUNGEN

1. HACKING: 1 , 3 , 4 , 5

2. EINSTELLUNGEN UND WOHLBEFINDEN: technische Sicherheit

3. PHISHING-ATTACKE: 1 (der Name ist nicht richtig geschrieben); allgemein wird auch abgeraten, die Anhänge von zweifelhaften E-Mails zu öffnen.

4. SPEICHERMEDIEN: 1 , 3 , 4

5. VERBREITUNG VON INFORMATIONEN:

- **Welche Informationen könnten Dritte aus diesem Foto herauslesen?**

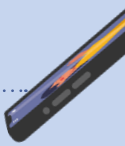
1 - 13; (die Fotos enthalten Metadaten, das heißt Informationen über das Foto und das Gerät, die mithilfe eines Bildverarbeitungsprogramms ausgelesen werden können).

- **All diese Daten zu teilen, ist nicht ohne Risiko. Was sind potenzielle Gefahren?**

1 - 4; Wilderer nutzen Social Media, um die Tötung bedrohter Tierarten zu planen. Nashörner sind wegen des Wertes ihres Horns besonders gefährdet.

6. BETRUG:

- Die Webseite verfügt nicht über eine sichere HTTPS-Verbindung.
- Der Verkaufspreis ist nicht realistisch.
- Man muss im Voraus bezahlen, um das Angebot zu erhalten.



7. DESINFORMATION: 1 - **www.bee-secure.lu/desinformation-politik**

8. ILLEGALE INHALTE: ja - **https://stopline.bee-secure.lu/de/illegalcontent**[29]

9. SEXTING : 2

10. CYBER-MOBBING: 1

KREUZWORTRÄTSEL: WAS HABEN SIE BEHALTEN?

1 Ich nutze einen **Manager**, um meine Passwörter sicher an einem Ort zu speichern.

2 Ich **deaktiviere** alle unnötigen Berechtigungen, um meine Daten zu schützen.

3 Ich bleibe **kritisch** gegenüber unbekannten E-Mails und Informationen im Netz.

4 Ich vermeide Online-Transaktionen im **öffentlichen WLAN**.

5 Auch wenn ich automatische Updates aktiviere und ein Antivirenprogramm habe, führe ich regelmäßig einen **manuellen Scan** auf meiner Festplatte durch.

6 Ich **verschlüssele** sensible Dokumente oder Daten, die in der Cloud gespeichert werden.

7 Unwissenheit schützt nicht vor **Strafe**.

8 Ich trage zum Kampf gegen illegale Inhalte bei, indem ich sie bei der BEE SEECURE **Stopline** melde.

9 Wenn ich Opfer einer ungewollten Veröffentlichung intimer Inhalte werde, sammle ich **Beweise**, um Anzeige zu erstatten.

10 Ich prüfe die **Vertrauenswürdigkeit** einer Webseite, bevor ich dort ein Produkt kaufe oder einen Service bestelle.

[29] Inhalte basierend auf einer wahren Geschichte: Diese Kommentare wurden 2015 gepostet; die Urheber wurden 2017 zu einer Geldstrafe zwischen 1000 und 1500 € verurteilt. www.rtl.lu/news/national/a/1036740.html

ZUSÄTZLICHE INFORMATIONEN UND MATERIALIEN

PUBLIKATIONEN

BEE SECURE veröffentlicht regelmäßig Inhalte zu Themen rund um eine sichere und verantwortungsbewusste Internetnutzung durch Kinder und Jugendliche, darunter Ratgeber, Thematische Beiträge, pädagogische Materialien sowie Berichte. Diese Publikationen finden Sie unter **www.bee-secure.lu/publikationen**.

TRAININGS

BEE SECURE bietet diverse Sensibilisierungstrainings für Kinder und Jugendliche, Fortbildungen für Lehrer und Erzieher sowie Elternabende an. Den aktuellen Katalog finden Sie auf **www.bee-secure.lu** im Bereich Trainings. Dort können Sie auch bei Interesse Trainingsangebote buchen.

BIBLIOGRAFIE

BEE SECURE. BEE SECURE RADAR 2022
www.bee-secure.lu/de/publikation/bee-secure-radar-2022 (zuletzt aufgerufen am 10/03/2022)

_____. BILDSCHIRME IN DER FAMILIE
www.bee-secure.lu/bildschirme-in-der-familie (zuletzt aufgerufen am 11/11/2021)

_____. CYBER-MOBBING
www.bee-secure.lu/fr/risques/cyberharcelement (zuletzt aufgerufen am 11/11/2021)

_____. DESINFORMATION
www.bee-secure.lu/de/risiken/desinformation (zuletzt aufgerufen am 11/11/2021)

_____. DÉSINFORMATION IN DER POLITIK
www.bee-secure.lu/desinformation-politik (zuletzt aufgerufen am 11/11/2021)

_____. NETIQUETTE
www.bee-secure.lu/netiquette (zuletzt aufgerufen am 11/11/2021)

_____. WAS IST BIG DATA ?
www.bee-secure.lu/de/publikation/was-ist-big-data (zuletzt aufgerufen am 11/11/2021)

_____. DSGVO (GDPR)
www.bee-secure.lu/de/publikation/datenschutzgrundverordnung-dsgvo (zuletzt aufgerufen am 11/11/2021)

BEE SECURE, CNPD, CYBERSECURITY COMPETENCE CENTER LUXEMBOURG (C3). SPAMBEE
https://spambee.lu (zuletzt aufgerufen am 11/11/2021)

BEE SECURE, SCRIPT, POLICE LËTZEBUERG, PARQUET DE LUXEMBOURG. NACKT IM NETZ?
www.bee-secure.lu/sexting-ratgeber (zuletzt aufgerufen am 11/11/2021)

BEE SECURE, TACTICAL TECH. RÉAGIR À UNE VIOLATION DE DONNÉES.
www.bee-secure.lu/fr/publication/comment-reagir-a-une-violation-de-donnees (zuletzt aufgerufen am 11/11/2021)

CORE. A KNOWLEDGE BASE ON CHILDREN &CHILDREN IN THE DIGITAL AGE.
www.core-evidence.eu (zuletzt aufgerufen am 10/03/2022)

COMMISSION NATIONALE POUR LA PROTECTION DE DONNÉES. CNPD
https://cnpd.public.lu/fr/commission-nationale.html (zuletzt aufgerufen am 11/11/2021)

_____. FORMULAIRE DE RÉCLAMATION
https://cnpd.public.lu/fr/particuliers/faire-valoir/formulaire-plainte.html (zuletzt aufgerufen am 11/11/2021)

_____. RÈGLEMENT GÉNÉRAL SUR LA PROTECTION DES DONNÉES
https://cnpd.public.lu/fr/dossiers-thematiques/Reglement-general-sur-la-protection-des-donnees.html (zuletzt aufgerufen am 11/11/2021)

CIRCL. formulaire de réclamation..
www.circl.lu/report/#report-an-incident (zuletzt aufgerufen am 11/11/2021)

DER POSTILLON. ERSTES BABY MIT MASKE GEBOREN.
www.der-postillon.com/2020/09/baby-maske.html (zuletzt aufgerufen am 11/11/2021)

ILR
https://web.ilr.lu (zuletzt aufgerufen am 11/11/2021)

LIVINGSTONE, S. & STOILOVA, M. (2021). THE 4CS:CLASSIFYING ONLINE RISK TO CHILDREN. (CO:RE SHORT REPORT SERIES ON KEY TOPICS). HAMBURG: LEIBNIZ-INSTITUT FÜR MEDIENFORSCHUNG | HANS-BREDOW-INSTITUT (HBI); CO:RE-CHILDREN ONLINE: RESEARCH AND EVIDENCE.
www.doi.org/10.21241/ssoar.71817 (zuletzt aufgerufen am 10/03/2022)

NBC NEWS. YOUR SAFARI SELFIES ARE CUTE, BUT THEY'RE A ROAD MAP FOR POACHERS.
www.nbcnews.com/business/business-news/your-safari-selfies-are-cute-they-re-road-map-poachers-n1016031 (zuletzt aufgerufen am 23/11/2021)

RTL. GELDSTROF FIR 3 UGEKLOTEN, PARQUET HAT FESTE PRISONG GEFROT
https://www.rtl.lu/news/national/a/1036740.html (zuletzt aufgerufen am 11/11/2021)

TACTICAL TECH. LA TECHNOLOGIE EST STUPIDE : COMMENT CHOISIR LA TECHNOLOGIE POUR LE TRAVAIL À DISTANCE ?
https://tacticaltech.org/news/technologie-est-stupide (zuletzt aufgerufen am 23/11/2021)

ULC. VOTRE ASBL
www.ulc.lu/fr/presentation/?id=1 (zuletzt aufgerufen am 11/11/2021)

Was sind Ihrer Meinung nach die Lösungen?

1. Hacking

Helfen Sie Lynn, angemessen zu reagieren, indem Sie aus den folgenden Handlungen auswählen:

- ○ 1
- ○ 2
- ○ 3
- ○ 4
- ○ 5

2. Einstellungen und Wohlbefinden:

Lara möchte negative Auswirkungen von Bildschirmzeit auf ihr Wohlbefinden bestmöglich vermeiden. Dazu hat sie beschlossen:

_ _ C _ _ _ _ _ _ E
S _ _ _ _ _ _ _ _ T
BERÜCKSICHTIGEN!

3. Phishing-Attacke:

Helfen Sie Dennis, die Risiken zu erkennen:

- ○ 1
- ○ 2

4. Speichermedien

Helfen Sie Julie, ihr Speichersystem zu diversifizieren:

- ○ 1
- ○ 2
- ○ 3
- ○ 4

5. Verbreitung von Informationen (1/2)

Welche Informationen könnten Dritte aus diesem Foto herauslesen?

- ○ 1
- ○ 2
- ○ 3
- ○ 4
- ○ 5
- ○ 6
- ○ 7
- ○ 8
- ○ 9
- ○ 10
- ○ 11
- ○ 12
- ○ 13

5. Verbreitung von Informationen (2/2)

All diese Daten zu teilen, ist nicht ohne Risiko. Was sind potenzielle Gefahren?

○ 1 ○ 3
○ 2 ○ 4

6. Betrug

Helfen Sie Sasha dabei, zu verstehen, dass es sich um Abzocke handelt! Was sind die sichtbaren Indikatoren auf der Webseite?

Kreisen Sie auf der Webseite die entsprechenden Bereiche ein.

7. Desinformation

Helfen Sie Pierre dabei, die Risiken der Desinformation zu verstehen:

○ 1 ○ 2

8. Illegale Inhalte

Ist ein solches Verhalten im Internet strafbar?

○ 1 ○ 2

9. Sexting

Darf Pascal aus rechtlicher Sicht ein intimes Foto von sich selbst teilen?

○ 1 ○ 3
○ 2 ○ 4

10. Cyber-Mobbing

Denis weiß nicht, was er tun soll. Was raten Sie ihm?

○ 1 ○ 2

Weitere Informationen finden Sie auf **bee-secure.lu**

Éditeur : Service national de la jeunesse (SNJ)
B.P. 707 · L-2017 Luxembourg
www.snj.lu
www.bee-secure.lu

Initié par :
LE GOUVERNEMENT DU GRAND-DUCHÉ DE LUXEMBOURG

Opéré par :
Service national de la jeunesse
KJT

Cofinancé par :
Cofinancé par le mécanisme pour l'interconnexion en Europe de l'Union européenne

Version digitale
Risques sur Internet – 03.2022
ISBN : 978-2-919796-46-5

© Conception graphique : Alternatives communication