

Datum: 05.02.2024
Autor: René Johansen,

**Didaktisch-methodische Hinweise zum
Live Hacking
SID 2024**
Freistaat Sachsen
Landesamt für Schule und Bildung



Online am Limit - dein Netz. dein Leben. deine Grenzen.

Safer Internet Day 2024

Arbeitsmaterial für Lehrer

**Didaktisch - methodische Hinweise
zur Online-Veranstaltung
Freistaat Sachsen - SID 2024**

Landesamt für Schule und Bildung (LaSuB)

René Johansen

Im Auftrag von ML Consulting GmbH, Köln

Inhaltsverzeichnis

1	Organisatorisches	4
1.1	Veranstaltungsplanung.....	4
1.2	Veranstaltungssoftware	4
2	Didaktisch - methodische Hinweise zur Online-Veranstaltung „Online am Limit - dein Netz. dein Leben. deine Grenzen.“	5
2.1	Einführung.....	5
2.1.1	Zusammenfassung.....	5
2.1.2	Ziele	5
2.1.3	Fragen zur Vor- oder Nachbereitung	5
2.2	Die digitale Identität.....	6
2.2.1	Zusammenfassung.....	6
2.2.2	Ziele	6
2.2.3	Fragen zur Vor- oder Nachbereitung	6
2.2.4	Weiterführende Hinweise	6
2.3	Identitätsdiebstahl und Identitätsbetrug	6
2.3.1	Zusammenfassung.....	6
2.3.2	Ziele	7
2.3.3	Fragen zur Vor- oder Nachbereitung	7
2.3.4	Weiterführende Hinweise	7
2.4	Künstliche Intelligenz und Deepfake.....	7
2.4.1	Zusammenfassung.....	7
2.4.2	Ziele	8
2.4.3	Fragen zur Vor- oder Nachbereitung	8
2.4.4	Weiterführende Hinweise	8
2.5	Meet Lilly Munipula!.....	8
2.5.1	Zusammenfassung.....	8
2.5.2	Ziele	9
2.6	Woran sind Deepfakes zu erkennen?.....	9
2.6.1	Zusammenfassung.....	9
2.6.2	Ziele	10
2.6.3	Fragen zur Vor- oder Nachbereitung	10
2.6.4	Weiterführende Hinweise	10

2.7	Schutzmaßnahmen: Was tun bei Verdacht oder als Opfer eines Identitätsdiebstahls?	11
2.7.1	Zusammenfassung	11
2.7.2	Ziele	11
2.7.3	Fragen zur Vor- oder Nachbereitung	11
2.7.4	Weiterführende Hinweise	11
2.8	Schutzmaßnahmen: 5 Goldene Regeln zum Schutz vor Identitätsdiebstahl	12
2.8.1	Zusammenfassung	12
2.8.2	Ziele	12
2.8.3	Fragen zur Vor- oder Nachbereitung	12
2.8.4	Weiterführende Hinweise	12
2.9	Zusammenfassung, Fragen und Antworten	12

Historie

01.02.2024	René Johansen	Ersterstellung
05.02.2024	René Johansen	Fertigstellung

1 Organisatorisches

1.1 Veranstaltungsplanung

Safer Internet Day (SID) am 06.02.2024,
2 Veranstaltungen für Schüler zu je 1h
1 Veranstaltung für Lehrer 1,5h

1. Veranstaltung: 09.00-10.00 Uhr
2. Veranstaltung: 10.30-11.30 Uhr
3. Veranstaltung: 14.00-15.30 Uhr

Die Veranstaltung wird durch PowerPoint-Folien begleitet.
Der Foliensatz kann im PDF-Format bei LaSuB Sachsen angefordert werden.

1.2 Veranstaltungssoftware

Veranstaltungsformat: Cisco Webex

Hinweise zur optimalen Nutzung von Cisco Webex im Verlauf der Live-Hacking-Veranstaltung:

Nutzen Sie nach Möglichkeit den Browser Google Chrome.

Ziel der nachfolgenden Hinweise ist es, Sie in die Lage zu versetzen, der Veranstaltung so folgen zu können, dass das Video des Gastgebers angezeigt („auf der Bühne“, „im Bereich“) bleibt und nicht je nach Sprecher wechselt.

Achtung: In neueren Versionen von Webex (wir beziehen uns als „neue Version“ auf Version 44) haben sich Begrifflichkeiten geändert, der Vorgang bleibt aber ähnlich.

- Nachdem Sie sich über den bereitgestellten Link in die Veranstaltung eingeloggt haben, öffnen Sie bitte die Teilnehmerliste (Symbol unten rechts, links neben dem Chat-Symbol)
Neue Version: Teilnehmerbereich öffnen.
- Klicken Sie auf „Gastgeber“ (Felix Wabra). Bringen Sie den Gastgeber „auf die Bühne“.
Neue Version „In Bereich ziehen“)
- Schließen Sie die Teilnehmerliste.
- Wechseln Sie nun zum Menü „Layout“ (oben rechts).
- Wählen sie die Option „Stapel“.
- Aktivieren Sie „Vollbild“.
- **Deaktivieren** Sie „Aktiven Sprecher auf der Bühne anzeigen“.
Neue Version: **Personenfokus deaktivieren**.

Nun bleibt der Fokus auf dem Gastgeber bzw. den Präsentierenden, unabhängig davon, wer spricht.

2 Didaktisch - methodische Hinweise zur Online-Veranstaltung „Online am Limit - dein Netz. dein Leben. deine Grenzen.“

2.1 Einführung

2.1.1 Zusammenfassung

Einführungstext

Identitätsdiebstahl und Identitätsbetrug sind weitverbreitet und haben viele Gesichter. In jedem dieser Fälle aber geben Cyberkriminelle sich im Internet als eine andere Person aus.

Die Folgen können schwerwiegend sein – von finanziellen Schäden über Rufschädigung bis zu strafrechtlichen Konsequenzen.

Dazu kommt: unsere digitale Identität ist seit der Entwicklung von künstlicher Intelligenz und dem Einsatz von Deepfakes gefährdeter denn je.

Diese Live-Hacking-Veranstaltung klärt Schüler anhand nachvollziehbarer Vergleiche und Beispiele über digitale Identität und deren Missbrauch auf.

Die Dozenten demonstrieren, wie Angreifer künstliche Intelligenz einsetzen, um ihre Ziele zu erreichen und erläutern, wie einfach umzusetzende Maßnahmen dabei helfen, sich vor Identitätsdiebstahl und Identitätsbetrug zu schützen.

Vorspann

- Hinweise zur Nutzung von Webex (siehe Abschnitt 1.2 Veranstaltungssoftware)
- Vorstellung der Durchführenden
- Vorstellung des Ablaufs (siehe Übersicht im Foliensatz)

2.1.2 Ziele

Die Schüler erhalten einen Überblick über den Inhalt der Veranstaltung sowie über den zur Durchführung beauftragten Bildungsdienstleister ML Consulting Schulung und Support GmbH und die durchführenden Dozenten.

Die Themen „Identität“, „Digitale Identität“, „Identitätsdiebstahl“ und „Identitätsbetrug“ werden aus dem Motto „Online am Limit - dein Netz. dein Leben. deine Grenzen.“ heraus entwickelt und mit dem Thema „Künstliche Intelligenz“ verbunden.

2.1.3 Fragen zur Vor- oder Nachbereitung

- Wie würdest du das Motto unserer Veranstaltung für den SID 2024 in Sachsen „Online am Limit - dein Netz. dein Leben. deine Grenzen“ verstehen?
- Wie würdest du diesen Leitgedanken einem jüngeren Mitschüler mit möglichst einfachen Worten erklären?

2.2 Die digitale Identität

2.2.1 Zusammenfassung

Ausgehend vom Leitgedanken unserer Veranstaltung für den SID 2024 im Freistaat Sachsen greifen wir das Thema „Digitale Identität“ genauer auf. Den Schülern wird mit naheliegenden Vergleichen ihre digitale Identität veranschaulicht und es wird verdeutlicht, dass diese einerseits gepflegt, andererseits aber auch geschützt und gegebenenfalls verteidigt werden muss.

Es wird beispielhaft benannt, was die Identität einer Person im realen Leben mit der digitalen Identität im Netz verbindet und woraus letztere sich zusammensetzt.

2.2.2 Ziele

Den Schülern wird bewusst gemacht, dass jeder mit Zugang zum Internet auch eine digitale Identität hat. Die Teilhabe am Internet eröffnet scheinbar grenzenlose Möglichkeiten, macht uns aber auch verwundbar, vor allem, was den Missbrauch unserer digitalen Identität betrifft.

2.2.3 Fragen zur Vor- oder Nachbereitung

- Welche persönlichen Informationen könnten Teil deiner digitalen Identität sein?
- Welche Vorteile bietet eine starke digitale Identität?
- Gibt es Deiner Meinung nach Personengruppen, die in heutiger Zeit keine digitale Identität besitzen? Auf wen könnte das zutreffen?

2.2.4 Weiterführende Hinweise

Eine einfache Einführung in Datenschutzgesetze und die Bedeutung der Einhaltung dieser Gesetze könnte den Schülern ein Verständnis für ihre Rechte in der digitalen Welt vermitteln.

2.3 Identitätsdiebstahl und Identitätsbetrug

2.3.1 Zusammenfassung

Unsere digitalen Spuren werden von vielen Unternehmen genutzt, um personalisierte Dienste oder Werbung anzubieten. Wir weisen in diesem Zusammenhang darauf hin, dass es u.a. deshalb ratsam ist, bewusst mit Online-Aktivitäten umzugehen und sicherzustellen, dass die eigenen digitalen Spuren eine positive digitale Identität widerspiegeln.

Anders aber verhält es sich bei Identitätsdiebstahl. Sensible Daten werden in betrügerischer Absicht gestohlen. Die Vorgehensweise wird an zwei Beispielen erläutert.

Beispiel 1: Holzwickede, Januar 2023. Schüler der Josef-Reding-Hauptschule wurden über Tiktok und Instagram von den Profilen verschiedener Lehrer angeschrieben. Diese Profile stellten sich als unecht heraus.¹

Beispiel 2: Twitter-Kanal Azusagakuyuki von Yasuo Nakajima. Der 50-jährige Japaner gab sich 2019 auf Twitter mittels manipulierter Bilder als junges, motorradbegeistertes Mädchen mit

¹ <https://www.hellwegeranzeiger.de/holzwickede/tiktok-und-instagram-unbekannte-erstellen-fake-profile-von-holzwickeder-lehrern-w684694-1000722356/>

langen wehenden Haaren aus. Er postete Aufnahmen, die ihm zehntausende Follower einbrachten. Immerhin, die Haare waren echt.

2.3.2 Ziele

Die Schüler lernen, was Identitätsdiebstahl und Identitätsbetrug sind und wie diese sich unterscheiden. Mehrere reale Vorkommnisse im Story-Format sollen einen Einblick geben, welche Gründe zu Identitätsdiebstahl führen und wie sich Identitätsbetrug auf die Opfer auswirkt.

2.3.3 Fragen zur Vor- oder Nachbereitung

- Was ist Identitätsbetrug und wie unterscheidet dieser sich von Identitätsdiebstahl? Diese Frage prüft das grundlegende Verständnis der Schüler für beide Begriffe.
- Welche Arten von persönlichen Informationen könnten bei einem Identitätsbetrug gestohlen oder verwendet werden?

2.3.4 Weiterführende Hinweise

Geschichten oder Fallstudien über reale Fälle von digitalen Identitätsdiebstählen können den Schülern verdeutlichen, welche Auswirkungen unsicheres Online-Verhalten haben kann.²

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) bezeichnet in seinem Lagebericht 2023 Identitätsdiebstahl als Hauptbedrohung für die Zielgruppe „Gesellschaft“. Für die Zielgruppen „Wirtschaft“ sowie „Staat und Verwaltung“ wird vom BSI-Lagebericht Ransomware als Top-Bedrohung beschrieben.³

Identitätsdiebstahl wird inzwischen durch Cyberkriminelle auch als Dienstleistung mit Phishing-as-a-Service (PhaaS) vermarktet. In diesem Modell kaufen potenzielle Angreifer buchstäblich "Phishing-Dienste" von Hackern oder kriminellen Gruppen, die ihre Expertise und Tools bereitstellen, um betrügerische Aktivitäten durchzuführen.

Zusätzlich wäre für interessierte Schüler auch das Thema „Information Stealer“ von Interesse. Information Stealer sind schädliche Softwareprogramme, die darauf abzielen, vertrauliche Informationen von Computern oder Geräten zu stehlen. Diese Art von Malware ist darauf spezialisiert, persönliche und sensible Daten zu extrahieren, um sie dann an Angreifer oder Kriminelle zu übermitteln. Die gestohlenen Daten umfassen auch Cookies und biometrische Daten, wie zum Beispiel Fingerabdrücke. Die entwendeten Anmeldeinformationen bieten Cyberkriminelle anschließend auf Marktplätzen im Darknet zum Verkauf an.

2.4 Künstliche Intelligenz und Deepfake

2.4.1 Zusammenfassung

Um Identitätsdiebstahl und -betrug anschaulich zu demonstrieren, leiten die Dozenten zu KI und Deepfakes über. Auch in diesem Fall wird anhand von für Schüler gut nachvollziehbaren Vergleichen beschrieben, was KI und Deepfake ausmachen. Dabei greifen die Dozenten aus Demonstrationszwecken direkt auf KI, in diesem Fall ChatGPT, zurück:

² <https://www.verbraucherzentrale.de/wissen/digitale-welt/datenschutz/welche-folgen-identitaetsdiebstahl-im-internet-haben-kann-17750>
<https://www.checked4you.de/computer-internet/social-media/wenn-ein-facebook-freund-dein-neuer-freund-sein-will-351190>

³ BSI Lagebericht 2023, Seite 47, Seite 51

Frage an ChatGTP: „Was ist künstliche Intelligenz, für einen Schüler oder Heranwachsenden beschrieben?“

ChatGTP: „Stell dir vor, künstliche Intelligenz (KI) ist wie ein super-schlauer Roboter-Freund. Dieser Roboter kann lernen, Dinge zu verstehen, wie wenn du ihm bebringst, welche Farbe Äpfel haben. Mit der Zeit wird der Roboter so klug, dass er von selbst Äpfel erkennen kann, ohne dass du es ihm jedes Mal sagen musst. Genau wie ein Freund, der immer schlauer wird.“

Der für das Hacking zuständige Dozent leitet dann auf Deepfake über und erklärt, wie künstliche Intelligenz dabei helfen kann, auf Bildern, in Videos und selbst in live durchgeführten Videokonferenzen den Anschein von Authentizität zu wecken.

2.4.2 Ziele

Künstliche Intelligenz und Deepfake werden durch Beispiele und in ihrer Wirkung demonstriert. Damit wird den Schülern das Potenzial dieser Anwendungen vor Augen geführt – im Einsatz für positive Zwecke als auch für möglichen Missbrauch. Gleichzeitig erfolgt die Vorbereitung für die nun folgenden Live-Hacking-Szenarien.

2.4.3 Fragen zur Vor- oder Nachbereitung

- Kannst du Beispiele für den Einsatz von künstlicher Intelligenz im Alltag nennen?
- Welche ethischen Überlegungen sind bei der Entwicklung und Anwendung von künstlicher Intelligenz wichtig? Diese Frage zielt darauf ab, das Bewusstsein der Schüler für die ethischen Aspekte von künstlicher Intelligenz zu schärfen, einschließlich Fragen der Privatsphäre, Diskriminierung und Verantwortlichkeit.

2.4.4 Weiterführende Hinweise

Das BSI hat im Lagebericht 2023 künstliche Intelligenz unter „Herausgehobenen Trend in der IT-Sicherheit“ erfasst und als eine der Schlüsseltechnologien der Digitalisierung“ bezeichnet.⁴: „Egal, ob ein Text geschrieben oder ein Bild kreiert werden soll, künstliche Intelligenz ist inzwischen so weit, dass das Ergebnis kaum noch von dem eines Menschen zu unterscheiden ist – und das mit großer Zeitersparnis.“

2.5 Meet Lilly Munipula!

2.5.1 Zusammenfassung

Ausgangslage: Es geht um Mike Clueless, einen Fan der Influencerin Lilly Munipula. Mike weiß nicht, dass Felix, der Hacker, noch eine Rechnung mit ihm offen hat und versuchen wird, Mike's digitale Identität zu übernehmen und für eigene Zwecke zu missbrauchen.

Mike's Profil auf Instagram ist allerdings privat und gut abgesichert.

Felix weiß, dass Mike ein großer Fan von Lilly ist. Der Zufall kommt ihm zu Hilfe: Lilly Munipula bringt eine neue Single heraus, die sie den ersten Tausend Followern auf ihrer neuen Instagram-Seite kostenfrei zum Download anbieten wird, und das nur heute, von 12 bis 16 Uhr.

An Lill's Daten zu kommen ist einfach. Deren Facebook-Profil ist öffentlich.

Schritt 1:Felix bedient sich aus dem öffentlichen Profil von Lilly Munipula (TikTok, Facebook) und lädt sich Bilder und Videos herunter.

⁴ BSI. Lagebericht 2023, Abschnitt 10 Künstliche Intelligenz, Seite 71.

2. Schritt: Der Angreifer benutzt die kopierten Daten, um ein gefälschtes Profil von Lilly Munipula aufzubauen und auf Instagram zu veröffentlichen (Identitätsdiebstahl).

3. Schritt: Der Angreifer schreibt Mike unter gefälschtem Absender im Namen von Lilly Munipula an und fordert ihn auf, den beigelegten Link zu Instagram anzuklicken, um sich auf dem Profil von Lilly als Follower anzumelden und die Single kostenfrei downloaden zu können (Identitätsbetrug und Phishing).

4. Schritt: Mike ist misstrauisch. Er traut weder Absender noch Link. Er macht aber einen gravierenden Fehler: Er antwortet dem Absender und fragt nach einem Nachweis der Identität. Mike weiß von Lilly's Veröffentlichungen auf TikTok, dass Lilly vor 2 Wochen mit ihrem Golden Retriever in der Karibik war. Bilder gab es keine. Er bittet darum, ihm ein Bild von diesem Urlaub als Nachweis der Echtheit zu senden.

5. Schritt: Der Angreifer generiert das gewünschte Bild mit Deepfake. Darauf sind Lilly mit ihrem Hund am Meer zu sehen. Und das gleich mehrfach.

Um die Leistungsfähigkeit und Überzeugungskraft der generierten Bilder zu zeigen, können die Schüler selbst im Chat Bilder anfragen, die in Echtzeit generiert werden.

6. Schritt: Mike ist nun doch überzeugt, es mit der echten Lilly Manipula zu tun zu haben und klickt auf den beigelegten Link.

7. Schritt: Mike kann sich im 2. Anlauf in Instagram einloggen. Im ersten Anlauf aber schien die Anmeldung nicht zu funktionieren. In Wirklichkeit wurden bereits im ersten Anlauf die Log-in-Daten von Mike an den Angreifer übertragen.

8. Schritt: Der Angreifer übernimmt das Instagram-Account von Mike Clueless und missbraucht dessen Identität (Identitätsdiebstahl und Identitätsbetrug). Dies wird vom Angreifer demonstriert.

2.5.2 Ziele

Es wird an einem konkreten Beispiel dargelegt, was Deepfakes sind und wie diese gezielt für Angriffe eingesetzt werden können.

Die Schüler werden in das Szenario einbezogen.

Nach der Demonstration wird herausgearbeitet, welche Fehler der Anwender gemacht hat und um welche Arten von Angriffen es sich gehandelt hat.

2.6 Woran sind Deepfakes zu erkennen?

2.6.1 Zusammenfassung

Es kann herausfordernd sein, Deepfakes zu erkennen, da sie oft sehr realistisch aussehen. Die Dozenten erläutern anhand von Beispielen, woran Deepfakes erkennbar sind:

1. **Ungewöhnliche Bewegungen oder Gesichtsausdrücke:** Wirken Bewegungen oder Gesichtsausdrücke der Person im Video natürlich oder nicht? Unnatürliche Bewegungen können ein Hinweis auf Deepfakes sein.
2. **Unstimmigkeiten im Hintergrund:** Auf verschwommene Bereiche oder Artefakte achten. Manchmal passen die hinzugefügten Elemente nicht perfekt zur Umgebung.

3. **Fokussierung auf Gesichtsbereich:** In vielen Deepfakes liegt der Fokus oft auf dem Gesicht der Person. Wenn der Rest des Videos unscharf ist oder weniger Aufmerksamkeit bekommt, könnte dies auf Manipulation hinweisen.
4. **Überprüfung der Quelle:** Wenn das Video von einer nicht vertrauenswürdigen Quelle stammt oder es keine klaren Informationen darüber gibt, wer es gemacht hat, ist Mißtrauen angebracht.
5. **Qualität des Videos:** Einige Deepfakes können in der Qualität schlechter sein als echte Videos. Auf Unschärfen, unscharfe Kanten oder andere Anomalien achten.
6. **Stimme und Tonlage:** Manchmal passen die Stimme oder die Tonlage nicht zum restlichen Verhalten der Person im Video. Das könnte darauf hindeuten, dass die Audioaufnahme manipuliert wurde.
7. **Bekannte Personen und Quellen prüfen:** Wenn das Video eine bekannte Person zeigt oder von einer vertrauenswürdigen Quelle stammt, sollten zusätzliche Quellen oder die offiziellen Social-Media-Konten geprüft werden, um die Echtheit zu bestätigen.

Die zunehmende Echtzeitfähigkeit von Deepfakes bewirkt, dass man in Onlinemeetings nicht mehr sicher sein kann, ob man mit einer realen Person, einem Angreifer oder sogar dem Avatar eines Chatbots kommuniziert.

2.6.2 Ziele

Nachdem Schüler selbst mithelfen konnten, Deepfakes zu generieren, wird es ihnen leichter fallen, reale von generierten Bildern, Videos oder Personen zu unterscheiden.

2.6.3 Fragen zur Vor- oder Nachbereitung

- Kannst du einige Techniken nennen, die bei der Erstellung von Deepfakes verwendet werden?
Diese Frage soll den Schüler dazu anregen, über die verschiedenen Techniken nachzudenken, die bei der Erstellung von Deepfakes, wie zum Beispiel Gesichtswechsel oder Sprachmanipulation, eingesetzt werden können.
- Welche Rolle können KI-Technologien bei der Erkennung von Deepfakes spielen?
Diese Frage zielt darauf ab, das Verständnis des Schülers für die Nutzung von künstlicher Intelligenz bei der Erkennung von Deepfakes zu fördern und wie diese Technologien dazu beitragen können.

2.6.4 Weiterführende Hinweise

Die Dozenten empfehlen, die neu erworbene Fähigkeit der Schüler zur Unterscheidung von Deepfakes im Unterricht anhand weiterer Beispiele auszubauen.

Das Bundesamt für Sicherheit in der Informationstechnik bietet zahlreiche Hintergrundinformationen zu den technischen Aspekten von Deepfakes und erläutert mögliche Erkennungsmerkmale.⁵ Die Dozenten empfehlen weiterhin die Informationen von klicksafe zu diesem Thema.⁶

⁵ https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Kuenstliche-Intelligenz/Deepfakes/deepfakes_node.html

⁶ <https://www.klicksafe.de/desinformation-und-meinung/deepfakes>

2.7 Schutzmaßnahmen: Was tun bei Verdacht oder als Opfer eines Identitätsdiebstahls?

2.7.1 Zusammenfassung

Schüler brauchen Unterstützung, wenn sie unmittelbar betroffen sind. Die Dozenten erläutern Schritt für Schritt was zu tun ist, sollte man den Verdacht auf Identitätsmissbrauch haben oder bereits Opfer von Identitätsbetrug geworden sein.

1. Ruhe bewahren und nicht in Panik geraten: Es ist wichtig, ruhig zu bleiben. Panik kann dazu führen, dass unüberlegte Entscheidungen getroffen werden.
2. Eltern bzw. Erziehungsberechtigte informieren. Eltern können den Schüler bei den nächsten Schritten unterstützen und notwendige Maßnahmen ergreifen.
3. Kontakt mit Online-Plattformen aufnehmen. Falls der Identitätsdiebstahl im Zusammenhang mit einem Online-Konto steht, sollten die Eltern oder der Schüler selbst den Kundensupport der Plattform kontaktieren. Viele Online-Dienste haben Verfahren zur Meldung von Identitätsdiebstahl.
4. Passwörter ändern. Alle Passwörter für Online-Konten, insbesondere das betroffene Konto, sind zu ändern. Siehe dazu die 5 Goldenen Regeln dieser Veranstaltung.
5. Antivirenschutz durchführen. Es muss sichergestellt werden, dass keine schädliche Software auf dem Betriebssystem vorhanden ist. Allerdings wird nicht jede Schadsoftware erkannt. Bleiben Zweifel, sollte der PC plattgemacht und neu aufgebaut werden.
6. Identitätsdiebstahl bei der Polizei melden.
7. Alles dokumentieren. Verdächtige E-Mails oder Nachrichten festhalten. Diese können hilfreich sein, um den Vorfall zu klären.
8. 5 Goldene Regeln berücksichtigen und aus Erfahrung lernen.

2.7.2 Ziele

Die Schüler sollten nun für die angesprochenen Themen sensibilisiert sein. Wird ein Vorfall frühzeitig bemerkt, ist ein strukturiertes Vorgehen nicht nur hilfreich, sondern unterstützt auch physiologisch, das Vorgefallene besser zu verarbeiten.

2.7.3 Fragen zur Vor- oder Nachbereitung

- Wie lässt sich feststellen, ob man Opfer von Identitätsbetrug geworden ist?

2.7.4 Weiterführende Hinweise

Weitere Aufklärung bieten u.a. Verbraucherzentralen (Beispiel Niedersachsen)⁷ oder die Landespolizei (Beispiel Brandenburg)⁸

⁷ <https://www.verbraucherzentrale-niedersachsen.de/themen/internet-telefon/datenschutz/tipps-gegen-identitaetsdiebstahl>

⁸ <https://polizei.brandenburg.de/seite/ich-wurde-opfer-eines-identitaetsdiebstals/56591>

2.8 Schutzmaßnahmen: 5 Goldene Regeln zum Schutz vor Identitätsdiebstahl

2.8.1 Zusammenfassung

Für einen wirksamen Schutz vor Identitätsdiebstahl und Identitätsbetrug führen die Dozenten fünf wichtige Maßnahmen auf:

1. **Starke Passwörter verwenden:** Es sollten Passwörter verwendet werden, die schwer zu erraten sind eine Mischung aus Buchstaben, Zahlen und Sonderzeichen (volle Komplexität).
2. **Zwei-Faktor-Authentifizierung (2FA) nutzen:** Die Zwei-Faktor-Authentifizierung nutzen, wenn möglich. Wir erläutern das Verfahren anhand von Beispielen.
3. **Vorsichtig mit persönlichen Informationen umgehen:** Sparsam mit persönlichen Informationen online umgehen (Datensparsamkeit).
4. **Phishing-Versuche erkennen und verhindern:** Auf Plausibilität (E-Mails, SMS etc.) achten. Vorsicht vor Anhängen und Links in E-Mails. Nach Möglichkeit nicht aus der E-Mail heraus handeln. URL's lesen und verstehen. Und schließlich: keine verkürzten URL's anklicken, aus denen es nicht erkennbar ist, auf welche Webseite sie weiterleiten.
5. **Aktuelle Software und Antivirenprogramme nutzen:** Software und Antivirenprogramme auf dem neuesten Stand halten.

2.8.2 Ziele

Es werden Maßnahmen genannt, die dazu dienen, im Vorfeld die eigene Identität – digital oder nicht – wirksam zu schützen.

2.8.3 Fragen zur Vor- oder Nachbereitung

- Wie erstellst du starke Passwörter?
- Kennst du eine Methode, wie sich viele starke Passwörter problemlos merken lassen?
- Wie kannst du Datenminimierung umsetzen?
- Ist dein Social-Media-Account öffentlich? Warum?

2.8.4 Weiterführende Hinweise

Das Thema 2FA wird u.a. in der Broschüre „Informationssicherheit an sächsischen Schulen“ des Lasub detailliert erläutert.

Weiterführende Informationen bietet „datenschutz-schule.info⁹, eine Seite, die sich zunächst an Schulen, Schulleitungen, Lehrkräfte, schulische Datenschutzbeauftragte in NRW, sonst aber an jeden richtet, der mit Schule und Datenschutz zu tun hat.

2.9 Zusammenfassung, Fragen und Antworten

Wir gehen auf Fragen ein, die im Verlauf der Veranstaltung nicht beantwortet werden konnten.

Abschließend weisen wir auf die Broschüre und die Checkliste „Informationssicherheit an sächsischen Schulen“¹⁰ hin.

⁹ <https://datenschutz-schule.info/tag/2fa/>

¹⁰ <https://publikationen.sachsen.de/bdb/artikel/39153>

Datum: 05.02.2024
Autor: René Johansen,

**Didaktisch-methodische Hinweise zum
Live Hacking**
SID 2024
Freistaat Sachsen
Landesamt für Schule und Bildung



Diese ist in einer neuen Ausgabe, Stand 22.01.2024, erschienen.
Hier sind vor allem die Abschnitte über Passwortsicherheit und Social Engineering für die von den Dozenten angesprochene Thematik relevant.