

FÜR PÄDAGOGINNEN UND PÄDAGOGEN

METHODEN DER CYBERKRIMINALITÄT



Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital • Sicher • BSI

Ablauf der Unterrichtseinheit

Phase	Inhalt	Sozial- / Aktionsform
Arbeitsblatt 1 Phishing und Schadprogramme (ca. 1,5 U-Std.)	Lesen des Einführungsbeispiels mit einer verdächtigen Mail (Phishing). Schadensszenarien werden diskutiert. Phishing wird gegen Schadsoftware abgegrenzt. Eine Infobox fasst bisherige Erkenntnisse zusammen und nennt Bereiche, die von Phishing betroffen sein können. Das Beispiel dient als Anstoß, damit Schülerinnen und Schüler über eigene Erfahrungen zum Thema Phishing berichten und sich dazu austauschen.	Lesen des Fallbeispiels, Begriffs- und Prinzipienklärung über Infobox, Erfahrungsbericht geben, Austausch im Plenum
Arbeitsblatt 2 Phishing & Co. (ca. 2,5 U-Std.)	Es wird genauer erarbeitet, wie Phishing funktioniert, was damit bezweckt wird und dass andere Kommunikationswege auch betroffen sind (Smishing, Quishing, Vishing). Die Jugendlichen informieren sich darüber, wie sie Phishing erkennen können und was sie im Verdachtsfall tun sollten. Merkmale und Schutzmaßnahmen werden in Auflistungen übersichtlich zusammengefasst.	Video, Bearbeitung von Informationsmaterialien, Gruppenarbeiten, zusammenfassende Praxistipps
Arbeitsblatt 3 Schadsoftware (ca. 1 – 1,5 U-Std.)	Beispielhaft für Trojaner werden Einsatzbereiche benannt und mögliche Schäden aufgeführt. Es erfolgt ein Überblick über wesentliche Arten und Funktionen von Schadprogrammen. Mögliche Wege zur Infektion von Endgeräten durch Schadprogramme werden aufgezeigt. Es folgen Tipps zum Erkennen von und zum Schutz vor Schadsoftware sowie für den Fall einer Infektion.	Lesen des Fallbeispiels, Informationsphase über Infobox, Videos, interaktive Übung, Gruppenarbeit
Arbeitsblatt 4 Identitätsdiebstahl (ca. 1 – 1,5 Std.)	Lesen und Besprechen eines Einführungsbeispiels, bei dem ein Betrüger mittels Identitätsdiebstahl finanziellen Schaden anrichten konnte. Informationen zum Schutz vor Identitätsdiebstahl. Zusammenfassende Praxistipps zur gesamten Unterrichtseinheit.	Lesen des Fallbeispiels, Bearbeitung im Plenum, Video, Praxistipps

Hintergrundinformationen zum Thema der Einheit und Lösungshinweise zu den Aufgaben

Einordnung der Unterrichtseinheit

Schutz gegen und das Wissen über Phishing, seine Unterarten und die Infektion mit Schadprogrammen über zugesandte Dateien oder Links sind neben dem allgemeinen Geräte- und Accountschutz unerlässlich für einen sicheren digitalen Alltag. Diese grundlegende Maxime muss den Schülerinnen und Schülern von Anfang an verdeutlicht werden. Nervige E-Mails füllen also nicht nur E-Mail-Postfächer und bahnen Betrugsversuche an, sondern infizieren oft auch das Empfängersystem mit einem Schadprogramm zum Ausspionieren persönlicher Daten: Phishing ist der Fachbegriff – ein Kunstwort, das sich aus „Passwort“ und „Fishing“ zusammensetzt. Das Fischen nach Passwörtern hört sich harmloser an, als es in der Realität tatsächlich ist. Denn Phishing steht am Anfang verschiedenartiger Delikte, die vom „einfachen“ Datendiebstahl über illegale Kontoabbuchungen bis hin zu Angriffen auf Kritische Infrastrukturen reichen. Gezieltes Phishing ist eine Straftat und kann böse Folgen für die Opfer haben. Mittlerweile gibt es mehrere Unterarten des Phishings – in Anlehnung an den Kommunikations- oder Medienkanal, auf dem diese auftreten. Solche Versuche lassen sich nicht mit einer einmalig eingerichteten Maßnahme verhindern. Stattdessen muss man kontinuierlich wachsam sein, auf verdächtige Nachrichten achten und auf diese nicht unbedacht eingehen.

Nicht nur Jugendliche, sondern durchaus auch viele Erwachsene sind sich der Tragweite oft nicht bewusst und unterliegen gleich mehreren Irrtümern:

1. Sie glauben, dass ihnen so etwas nicht passieren kann. Aber: Phishing-Angriffe können zwar gezielt durchgeführt werden, doch steht dabei nicht unbedingt jemand persönlich im Visier. Die meisten Phishing-Angriffe erfolgen in breiter, undifferenzierter Streuung und in der Erwartung der Absender, dass sie in einer für sie lohnenden Quote Erfolg haben werden. Diese Willkürlichkeit kann unbesehen jeden treffen.
2. Menschen glauben, dass ihre Geräte, Anwendungen und Daten für Betrüger nicht interessant genug sind. Die Schadensszenarien sind jedoch derart breit und differenziert, dass sich niemand sicher sein kann. Diese werden im Verlauf der Unterrichtseinheit über Beispiele erläutert.
3. Die Phishing-Mail im Postfach an sich richtet zunächst noch keinen Schaden an und viele Menschen glauben, dass sie nicht auf Phishing-Versuche hereinfallen werden. Doch die Betrüger verschicken mittlerweile sehr professionelle Mails (bzw. andere Nachrichten) und arbeiten mit Versprechen, Zeitdruck oder Androhungen, die viele nur schwer ignorieren können. Auch wer Phishing häufig erkennt, kann zufällig durch äußere Umstände wie Zeitdruck oder Unaufmerksamkeit in eine Situation kommen, in der eine Phishing-Mail plausibel erscheint. Downloads sind oft verlockend und es ist kaum erkennbar, dass sie in Wirklichkeit eine Schadsoftware transportieren.

Die Darstellung dieses Hintergrunds soll Sie als Lehrerin, Lehrer oder pädagogische Fachkraft dabei unterstützen, die Schülerinnen und Schüler zu überzeugen, dass sie sich unbedingt schützen müssen. Das erfordert ein Stück weit Verhaltensänderung und bedarf entsprechender Motivation. Deshalb steigt die Unterrichtseinheit nicht sofort ins fachliche Thema ein, sondern stellt voran, dass sich die Klasse bzw. Gruppe erst einmal in einem gemeinsamen Austausch mit dem Problem auseinandersetzt. Die drei aufgeführten Irrtümer können und sollten Sie geeignet in den Unterricht einbringen.

Zu den einzelnen Arbeitsblättern

Arbeitsblatt 1: Phishing und Schadprogramme

Der Einstieg erfolgt über ein fiktives Beispiel einer verdächtig nach Phishing aussehenden Mail. Es verwendet typische und offensichtliche Merkmale, um die Zuordnung zum Phishing schnell vornehmen zu können und sollte mit dem Hinweis verbunden werden, dass Phishing-Versuche mittlerweile deutlich besser getarnt sind. Das Beispiel veranschaulicht, dass Betrügende durchaus auch bei Schülerinnen und Schülern Möglichkeiten haben, sich einen Vorteil – in diesem Fall Geld – zu verschaffen.

Es folgt eine Infobox mit der Beschreibung des Prinzips und der Nennung weiterer Bereiche, in denen Phishing betrieben wird.

Im Anschluss wird sich im Plenum zu eigenen Erfahrungen ausgetauscht. Ziel sollte sein, dass die Schülerinnen und Schüler die Einsicht gewinnen, sich schützen zu wollen.

Arbeitsblatt 2: Phishing & Co.

Für guten Schutz sollten die Jugendlichen zunächst verstehen, wie Phishing funktioniert und welche Zwecke Angreifer im Grundsatz verfolgen. Das vermittelt ein kurzes Video. Sinnvoll wäre ein anschließender Austausch, bei dem die Lernenden den Videoinhalt in eigenen Worten wiedergeben.

Da neben Phishing auch Unterarten – wie Smishing per SMS, Quishing über QR-Codes, Vishing über Telefon – verbreitet sind, wird zu den Unterarten ein Informationstext des BSI in Gruppen bearbeitet. An anderer Stelle wurde bereits darauf verwiesen, dass die Unterrichtseinheit nicht die Vielfalt aller Phishing-Methoden behandeln kann. QR-Codes könnten jedoch weiter vertieft werden, da sie im Alltag weit verbreitet sind und es schwierig sein kann, die Seriosität des Publizierenden zu beurteilen.

Im Weiteren erfahren die Schülerinnen und Schüler, woran sie verdächtige Mails erkennen können, und erhalten Tipps, wie sie sich schützen können. Auch dazu verweist das Arbeitsblatt auf einen Informationstext des BSI, der mittels Gruppenarbeit zu bearbeiten ist. Es gilt herauszuarbeiten, dass der Schutz bei Phishing nicht darin besteht, keine betrügerischen Nachrichten zu erhalten, sondern nicht auf die Forderungen in den betreffenden Mails hereinzufallen.

Die zusammenfassenden Praxistipps am Ende des Arbeitsblattes unterstützen dabei, die von den Schülerinnen und Schülern erarbeiteten Erkenntnisse zu festigen. Prägnant und kurz können sie sich das Wichtigste auch noch einmal in einem YouTube-Short des BSI anschauen.

Arbeitsblatt 3: Schadsoftware verstehen und vorbeugen

Der klassische Fall bei Schadsoftware besteht aus der Infektion mit einem Infostealer. Ein Virenschutzprogramm bietet einen guten, aber keinen vollkommenen Schutz. Über die Presse erfahren wir immer wieder, dass Angreifer auf spektakuläre Weise große Firmen oder Behörden hacken und dort Systeme und Daten verschlüsseln, um Geld für die Freischaltung zu erpressen. Opfer eines solchen gezielten Vorgangs werden kaum Jugendliche sein. Dennoch müssen auch sie mit dem Thema vertraut gemacht werden.

Das Arbeitsblatt beginnt mit einem Einführungsbeispiel aus der Lebenswelt der Jugendlichen: Es kann ihnen zum Beispiel passieren, dass sie eine vermeintlich tolle Mod für ein Spiel bekommen. In Wirklichkeit versteckt sich dahinter aber Adware, die viel Werbung einstreut und das Spiel extrem langsam macht oder ein Infostealer, der Zugangsdaten stiehlt. Weitere Schadensmöglichkeiten werden aus der sich anschließenden Übersicht über die grundlegenden Arten von Schadsoftware deutlich. Man kann sich leicht vorstellen, was eine Spyware anrichtet, die unbemerkt Mikrofon oder Kamera aktiviert. Das Eindringen eines Fremden in die Privatsphäre, das Ausspähen oder das Stehlen

von Daten soll vermieden werden. Hier bietet sich ein Aufgreifen der ersten Unterrichtseinheit an, in der es unter anderem um die Vergabe von Berechtigungen geht, die regeln, welche Apps worauf zugreifen dürfen.

Außerdem erarbeiten die Schülerinnen und Schüler Übersichten zum möglichen Schaden und zum Schutz vor Schadprogrammen. Auch Hinweise und Tipps für den Notfall werden zusammengestellt.

Arbeitsblatt 4: Identitätsdiebstahl

Dieses Arbeitsblatt erfüllt die Funktionen, den Identitätsdiebstahl im Kontext der Cyberkriminalität zu thematisieren und das zuvor Gelernte konkreter werden zu lassen. Die Jugendlichen wissen, wie sie mit Phishing-Nachrichten umgehen müssen. Sie bleiben aufmerksam und folgen keinen Aufforderungen zur Preisgabe von persönlichen Daten. Was aber könnte wirklich passieren, wenn der Phishing-Versuch und Identitätsdiebstahl erfolgreich war? Dann werden dem Angreifer sensible Daten übermittelt, zum Beispiel die im Arbeitsblatt erwähnten Bezahlcodes. Er kann die Daten betrügerisch nutzen und mit der fremden Identität, die er sich angeeignet hat, finanziellen Schaden anrichten.

Das Fallbeispiel ist bewusst komplexer ausgelegt. Ausgespäht wird zunächst das Smartphone von Jana. Sie wird nicht im Fokus des Angreifers gestanden haben, der vermutlich durch einen Zufallsfund über Jana an Daten von Freddi gelangt ist, auf dessen Kosten er dann den Betrug begeht. In dem Beispiel gibt es also zum einen einen Identitätsdiebstahl, dessen „Datenausbeute“ allein noch nicht reicht. Zum anderen fischt der Angreifer über eine zusätzliche Fake-Nachricht Zahlungsdaten von Freddi ab.

Das Beispiel sollte im Plenum besprochen werden, wozu die anschließende Aufgabe anleitet: mögliche Verständnisfragen klären, die Abläufe verstehen, wie Identitätsdiebstahl und Online-Shopping-Betrug funktionieren.

Für die Schülerinnen und Schüler dürfte auch besonders die Frage spannend sein, warum Freddi auf die Fake-Nachricht hereingefallen ist und seine Zahlungscodes an Jana weitergeschickt hat. Das greift zurück auf die Schutzmaßnahmen aus Arbeitsblatt 2. Die Jugendlichen können versuchen, diese am konkreten Fall anzuwenden und für Freddi zukünftige Verhaltenstipps zu entwickeln. Je geschickter der Betrüger agiert hat, umso schwieriger bis unmöglich war es für Freddi, zu erkennen, dass die Nachricht zwar von Janas Account kam, aber gar nicht von ihr stammte. Insofern sollte Freddi – und das gilt für uns alle – grundsätzlich keine Zahlungscodes weiterleiten.

Das anschließende Video des BSI mit Experteninterviews liefert fachliche Informationen zum Identitätsdiebstahl. Werden Identifikationsdaten entwendet, spricht man von **Identitätsdiebstahl**. Somit kann der Dieb im Namen des Bestohlenen handeln. Das wird durch **Social Engineering** noch unterstützt: Der Datendieb verschafft sich weitere Informationen über den Bestohlenen und kann so beispielsweise auch gegenüber nahestehenden Personen sehr authentisch auftreten.

Das Video geht zudem auf sichere Personalausweise ein. Vielfach gelangen Betrüger über unterschiedliche Möglichkeiten an die auf einem Personalausweis verzeichneten Daten. Bei der Verwendung des Ausweises im Netz sollte deshalb nur die offizielle Online-Funktion des Personalausweises verwendet werden. Diese ist durch eine Zwei-Faktor-Authentisierung (Besitz der Ausweiskarte und Zugriff auf den dort integrierten Chip über die NFC-Schnittstelle sowie Wissen der zugehörigen PIN) besonders gut geschützt.

Die abschließenden Tipps der Experten machen deutlich, wie wichtig online Aufmerksamkeit und überlegtes Handeln sind. Die Jugendlichen sollen diese Tipps in ihren eigenen Worten zusammenfassen. Die Praxistipp-Box am Ende des Arbeitsblattes kann als Kontrolle dienen.

Weiterführende Links

1. Phishing - how much is the phish!?

https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Cyber-Sicherheitslage/Methoden-der-Cyber-Kriminalitaet/Spam-Phishing-Co/Passwortdiebstahl-durch-Phishing/passwortdiebstahl-durch-phishing_node.html



2. Wie schützt man sich gegen Phishing?

https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Cyber-Sicherheitslage/Methoden-der-Cyber-Kriminalitaet/Spam-Phishing-Co/Passwortdiebstahl-durch-Phishing/Schutz-gegen-Phishing/schutz-gegen-phishing_node.html



3. Wie erkenne ich Phishing-E-Mails und -Webseiten?

https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Cyber-Sicherheitslage/Methoden-der-Cyber-Kriminalitaet/Spam-Phishing-Co/Passwortdiebstahl-durch-Phishing/Wie-erkenne-ich-Phishing-in-E-Mails-und-auf-Webseiten/wie-erkenne-ich-phishing-in-e-mails-und-auf-webseiten_node.html



4. Phishing – Checkliste für den Ernstfall:

https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/Wegweiser_Checklisten_Flyer/Checkliste_BSI_ProPK_Phishing.pdf?__blob=publicationFile&v=4



5. Schadprogramme – Fragen & Antworten:

https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Cyber-Sicherheitslage/Methoden-der-Cyber-Kriminalitaet/Schadprogramme/schadprogramme_node.html



6. So schützen Sie sich vor digitalem Identitätsdiebstahl und gehackten Accounts:

https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Cyber-Sicherheitslage/Methoden-der-Cyber-Kriminalitaet/Identitaetsdiebstahl/Schutzmassnahmen/schutzmassnahmen_node.html



7. „Update verfügbar/Ein Podcast des BSI #29: Phishing, Smishing, Quishing & Co. – Das BKA ermittelt“:

<https://www.youtube.com/watch?v=KJOTIofG4UI&list=PLUEPo9QCKRA6TIFi0IUbF8oXvqmORoq4q&index=23>



8. „Update verfügbar/Ein Podcast des BSUI #49: Alarmstufe Rot für private Daten – Schutz vor Identitätsdiebstahl“:

<https://www.youtube.com/watch?v=ALeJN96zEN8&t=2s>



Nachstehende Bedingungen regeln die zulässige Nutzung dieses Dokuments.

- (1) Die Bereitstellung erfolgt unter der Creative Commons Lizenz CC BY abrufbar unter <https://creativecommons.org/licenses/by/4.0/deed.de>, die durch diese Nutzungsbedingungen ergänzt wird.
- (2) Die Inhalte dieses Dokuments dürfen in jedwedem Format oder Medium vervielfältigt und weiterverbreitet werden. Die Inhalte dürfen verändert, ergänzt oder nur in Teilen genutzt werden. Bei der Verwendung dieses Dokuments ist in angemessener Weise (z. B. durch Verlinkung) auf diese Nutzungsbedingungen hinzuweisen.
- (3) Jegliche Verwendung dieses Dokuments darf in keinem Fall den Eindruck einer Zusammenarbeit mit dem BSI oder eines hoheitlichen Internetauftritts erwecken.
- (4) Internet-Seiten und andere Medien, in denen dieses Dokument verwendet wird, dürfen keine strafbaren, gewalttätigen oder sexuellen Inhalte darbieten.
- (5) Die Wiedergabe von abgebildeten Texten und Grafiken dieses Dokuments als Zitat ist ohne Zustimmung des BSI zulässig, soweit Sinn und Zusammenhang gewahrt bleiben. Die Wiedergabe von Aussagen des BSI muss wortgetreu und in Anführungszeichen erfolgen. In allen Fällen ist ein Quellennachweis aufzunehmen.
- (6) Das Logo des BSI enthält mit dem Bundesadler ein Hoheitszeichen, das durch § 124 OWiG und § 145 Abs. 1 Nr. 1 MarkenG geschützt ist und nur mit schriftlicher Zustimmung des BSI verwendet werden darf. Eine Freigabe für die Nutzung von BSI-Inhalten umfasst nicht die Verwendung des BSI-Logos.
- (7) Das BSI übernimmt in Bezug auf die Inhalte dieses Dokuments keine Garantie. Insbesondere wird keine Garantie für die Aktualität, Richtigkeit, Vollständigkeit oder dauerhafte Verfügbarkeit des Dokuments übernommen.
- (8) Die Einräumung von Rechten nach diesen Nutzungsbedingungen erfolgt unter Ausschluss der Gewährleistung (insb. Freiheit des Dokuments von Sach- und Rechtsmängeln, Verwendbarkeit des Dokuments für einen bestimmten Zweck sowie die Vollständigkeit und Korrektheit des Dokuments). Dieser Gewährleistungsausschluss gilt nicht, sofern das BSI einen Mangel arglistig verschweigt oder soweit dem BSI Vorsatz oder grobe Fahrlässigkeit vorzuwerfen ist.
- (9) Das BSI haftet in Bezug auf Schäden aus der Verletzung des Lebens, des Körpers oder der Gesundheit nur, sofern dem BSI wenigstens Fahrlässigkeit vorzuwerfen ist, für sonstige Schäden nur bei grober Fahrlässigkeit oder Vorsatz, und übernimmt darüber hinaus keine freiwillige Haftung. Die Vorschrift des § 839 BGB bleibt unberührt.

Für Rückfragen steht das Service-Center des BSI (service-center@bsi.bund.de) zur Verfügung.

Impressum

Herausgeber:

Bundesamt für Sicherheit in der Informationstechnik - BSI

Godesberger Allee 87, 53175 Bonn

E-Mail: service-center@bsi.bund.de

Internet: www.bsi.bund.de

Service-Center: +49 (0) 800 274 1000

Stand: 09/2025

Didaktische Aufbereitung: Eduversum GmbH