

FÜR DEN UNTERRICHT

# METHODEN DER CYBERKRIMINALITÄT



Bundesamt  
für Sicherheit in der  
Informationstechnik

Deutschland  
Digital • Sicher • BSI



## AB 1: PHISHING UND SCHADPROGRAMME

### Einführungsbeispiel

Jana und Hannah spielen in einem Clan das Videospiel Clash of Clans. Jana ist geschickt, hat einen hohen Spielstand erreicht und einen Vorrat an Juwelen – der Währung dieses Spiels – angelegt. Heute hat sie eine E-Mail von einer Firma erhalten, die sie nicht kennt. Diese teilt mit, dass sie Juwelen gewonnen habe. Die Mail wirkt komisch und sie fragt deshalb Hannah, die sich besser als sie selbst mit Smartphones und Apps auskennt.



Jana: „Woher wissen die, dass ich Clash of Clans spiele, und kennen noch meine Mail-Adresse?“

Hannah: „Das wissen mindestens alle aus unserem Clan und die kennen auch deine E-Mail-Adresse.

Dahinter stecken aber bestimmt Cyberkriminelle und ein Datenklau. Die werden das auf gut Glück breit verschickt haben.“

Jana: „Haben die mir jetzt einen Trojaner geschickt?“

Hannah: „Eher nicht. Das hier sieht eher nach Phishing aus, und zwar nach einem ungeschickten. Das Logo stimmt nicht und es gibt Fehler. Sogar beim Namen des Spiels. Der Link hinter dem Button öffnet vermutlich eine Maske. Da sollst du dann bestimmt persönliche Daten und deinen PIN für das Spiel eintragen.“

Jana: „Aber warum? War es richtig, dass ich den Button nicht angeklickt habe?“

Hannah: „Ja, definitiv. Da kann Vieles dahinterstecken. Vielleicht jemand, der im größeren Stil Spiele mit hohen Ständen an sich zieht und dann verkauft. Oder du kriegst ein günstiges Kaufangebot für weitere Juwelen, die aber gefälscht sind bzw. die es gar nicht gibt, und das merkst du erst nach dem Bezahlen.“

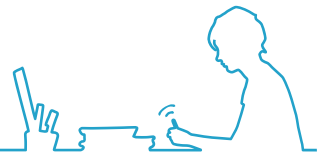
### PHISHING UND SCHADSOFTWARE

**Phishing** ist ein Kunstwort, das sich aus „Passwort“ und „Fishing“ zusammensetzt und so viel bedeutet wie „Fischen nach Passwörtern“. Beim **Phishing** erhält das Opfer Nachrichten über gängige Kommunikationswege, z. B. per E-Mail oder SMS. In der Nachricht wird die Empfängerin oder der Empfänger unter einem Vorwand aufgefordert, persönliche Daten preiszugeben oder Zahlungsdaten zu aktualisieren. Abgefischt werden meist persönliche Daten wie Kontaktinformationen, Passwörter oder Zahlungsdaten, die Angreifende für verschiedene Machenschaften nutzen wollen. Oft wollen sie an Geld herankommen. Sie verschicken die Mails an unzählige Empfänger und meist auf gut Glück, in der Hoffnung, dass irgendjemand darauf hereinfällt.

Ein weiteres Vorgehen von Angreifenden besteht darin, **Schadprogramme** auf die Geräte ihrer Opfer zu bringen, um sich darüber Zugang auf die Geräte zu verschaffen.



Analysiert zunächst in Zweiergruppen die Mail an Jana. Was findet ihr daran verdächtig? Tauscht euch dann in der Klasse darüber aus, wer schon einmal Phishing-Nachrichten erhalten hat und worum es dabei ging. Berichtet, wie ihr darauf reagiert habt.



## AB 2: PHISHING & CO.

Um uns zu schützen, sollten wir verstehen, wie Phishing funktioniert und was damit bezweckt wird.



**Schaut euch zu zweit das Video an. Tragt dann in der Klasse zusammen, wie Phishing funktioniert und was Angreifer damit erreichen wollen. Erklärt es in eigenen Worten.**

[https://multimedia.gsb.bund.de/BSI/Video/Sicher\\_im\\_Internet/Phishing.mp4](https://multimedia.gsb.bund.de/BSI/Video/Sicher_im_Internet/Phishing.mp4)



**Teilt euch in sechs Gruppen auf. Jeweils zwei Gruppen beschäftigen sich mit einem der drei Begriffe: Smishing, Quishing oder Vishing. Öffnet dazu den folgenden Link und erarbeitet eine kurze Erklärung zu eurem Begriff. Anschließend stellt eine Gruppe ihren Begriff im Plenum vor und die andere Gruppe ergänzt jeweils.**

[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](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)



### Phishing erkennen und sich schützen

Anfänglich waren Phishing-Mails recht einfach zu erkennen, wie in Janas Beispiel vom ersten Arbeitsblatt. Heute sind sie deutlich professioneller und besser gemacht. Ihr solltet deshalb bei allen Nachrichten aufmerksam sein und genau auf Form und Inhalt sowie den Absender der Nachricht achten.



**Bildet Gruppen mit jeweils vier Personen und bearbeitet eine der folgenden beiden Aufgaben mithilfe der Informationen aus dem Link.**

[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](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)

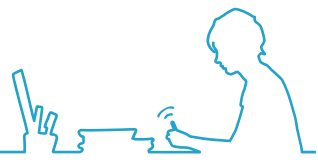


- Erstellt eine Liste mit Merkmalen, an denen ihr verdächtige Mails erkennen könnt.**
- Erstellt eine Liste mit Maßnahmen, wie ihr euch vor verdächtigen Mails schützen könnt und was ihr tun solltet, wenn ihr eine verdächtige Mail erhaltet.**

#### ZUSAMMENFASSENDE PRAXISTIPPS

- Sei aufmerksam, wenn Nachrichten „merkwürdig“ aussehen, sofortiges Handeln verlangen, tolle Versprechungen machen oder du Daten von dir preisgeben sollst.
- Gib niemals persönliche Daten wie Passwörter oder Zahlungsdaten über Messenger, E-Mail, SMS oder auf Social Media preis – egal, wie vertrauenserweckend die betreffende Nachricht erscheint. Frage im Zweifel eine erwachsene Vertrauensperson und lösche Mails und Nachrichten, die du als Phishing identifiziert hast.
- Schau dir das Short mit weiteren Tipps an: <https://www.youtube.com/shorts/rom2w8CW77I>.





## AB 3: SCHADSOFTWARE VERSTEHEN UND VORBEUGEN

### Einführungsbeispiel

Nach ihrem Gespräch über die Phishing-Mail reden Jana und Hannah weiter über Schadsoftware.

Jana: „Kann denn ein Trojaner, der sich im Anhang einer Mail versteckt, überhaupt Spiele infizieren?“

Hannah: „Klar. Trojaner sind getarnte Programme, die alle Apps angreifen können. Banking-Apps, Spiele und mehr. Bei Spielen tarnen sie sich zum Beispiel als coole Mod, Crack oder vermeintlicher Premiuminhalt und greifen deine Zugangsdaten ab. Wenn du Pech hast, klauen sie auch persönliche Informationen oder Kontodaten oder installieren weitere Schadprogramme.“

#### UNTERSCHIEDUNG VON ARTEN DER SCHADSOFTWARE UND IHRE AUSWIRKUNGEN

- **Schadsoftware** (engl. **Malware**) wird allgemein nach ihrem Angriffsziel unterschieden. In der Regel **tarnen** Angreifer die Schadsoftware als eine vertrauenswürdige Applikation oder führen sie **versteckt** im Hintergrund aus, um unbemerkt zu bleiben.
- **Adware** spielt auf dem infizierten Gerät unerwünschte Werbung aus.
- **Informationstealer**, kurz **Infostealer**, zielen auf den Diebstahl von personenbezogenen Daten und Zugangsdaten inkl. Passwörtern ab. Diese werden gesammelt und gebündelt ausgeleitet.
- **Spyware** tut das, was der Name sagt: **Überwachen**. Sie geht noch über einen Infostealer hinaus und hört vielleicht mit oder schaltet die Kamera unbemerkt ein. Sie sammelt auch Informationen über den Aufenthaltsort des infizierten Geräts.
- **Banking-Trojaner** zielen auf das Online-Banking ab. So versuchen Angreifer ungewollte Transaktionen unterzuschieben oder an Zugangsdaten für das Online-Banking zu gelangen.
- **Ransomware** sperrt den kompletten Zugriff auf das System oder verschlüsselt Daten. Für die Freigabe soll meist Lösegeld gezahlt werden.



#### Wie gelangt Schadsoftware auf Smartphones und andere Geräte und wie schützen wir uns?



Schaut euch zu zweit die beiden YouTube-Shorts an. Sie geben einen Überblick, wie man sich Schadsoftware einfangen kann und was dann zu tun ist.

<https://www.youtube.com/shorts/39X66epp2nU>

<https://www.youtube.com/shorts/WVj1lqalvTg>



Angriffswege und möglicher Schutz – Lies den folgenden Text in Einzelarbeit.

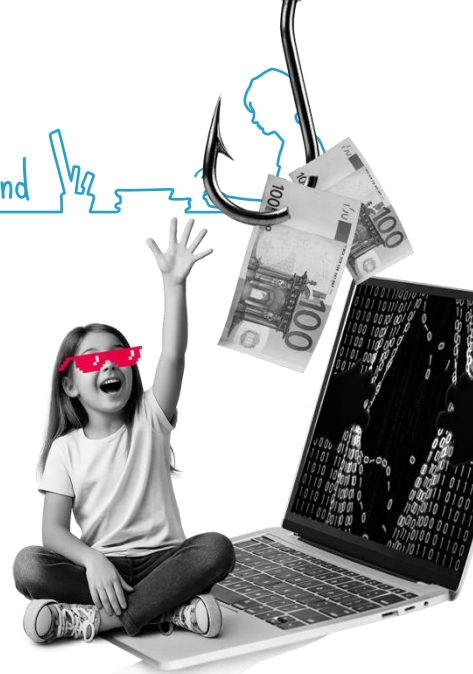
<https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Cyber-Sicherheitslage/Methoden-der-Cyber-Kriminalitaet/Schadprogramme/schadprogramme.html>



Wählt in Paarbeit einen der drei Abschnitte aus dem Text aus: „Was können Schadprogramme anrichten?“, „Wie schütze ich mich vor Schadprogrammen?“ oder „Was kann ich tun, wenn ich betroffen bin?“. Fasst die wichtigsten Informationen in Stichpunkten zusammen. Im Anschluss werden die Ergebnisse der Klasse vorgestellt.

## AB 4: IDENTITÄTSDIEBSTAHL

Beim Identitätsdiebstahl geben sich Kriminelle im Internet als eine andere Person aus. Die Folgen können schwerwiegend sein – von finanziellen Schäden über Rufschädigung bis zu strafrechtlichen Konsequenzen.



### Einführungsbeispiel

Jana erzählt Olli, dass ihr E-Mail-Account gehackt wurde – und darüber auch eines ihrer Social-Media-Profile, bei dem auch das Passwort über die Mail-Adresse geändert wurde. Dabei ist Freddi, ein gemeinsamer Bekannter, geschädigt worden. Was ist genau passiert? Der Hacker war ein richtiger Krimineller. Er hat die Handynummer von Freddi aus dem Smartphone von Jana ausgelesen. Dann hat er über Janas E-Mail-Account digitale Gutscheine, Konzert-Tickets und Online-Gaming-Guthaben bestellt und dabei Freddis Handynummer angegeben. Als Bezahlmethode hat er die Handyrechnung ausgewählt. Die Shops haben daraufhin Bezahlcodes per SMS an Freddi geschickt. Diese sollen zur Sicherheit und zum Abschluss der Bestellungen eingegeben werden. Der Hacker hat dann in Janas Namen eine Nachricht an Freddi geschickt, dass ihr Handy gerade Probleme beim Empfangen von SMS habe und sie auf Freigabecodes für Spiele warte. Angeblich habe sie die Codes an ihn senden lassen, er solle sie ihr bitte weiterschicken. Freddi hat sich nichts dabei gedacht und sie weitergeleitet – direkt in die Hände des Kriminellen im gekaperten Account. Dieser konnten die Bestellung damit abschließen. Die Rechnung ging an Freddi. Er war entsetzt. Schnell hat sich zwar geklärt, dass Jana davon nichts gewusst hat und nicht sie um die Weiterleitung gebeten hatte, aber ein Schaden ist trotzdem entstanden.



1. **Besprecht das Beispiel in der Klasse und klärt Verständnisfragen. Worin besteht der Identitätsdiebstahl? Worin besteht der Online-Shopping-Betrug?**
2. **Diskutiert, warum Freddi die Codes weitergeschickt hat. Wie könnte man sich schützen?**



**Vertieft das Thema, indem ihr euch zunächst zu zweit das folgende Video anschaut.**

**Stellt im Anschluss gemeinsam auf einem Plakat zusammen, was in dem Video zum Schutz gegen Schäden aus einem Identitätsdiebstahl genannt wird.**

[https://www.youtube.com/watch?v=uuXL5WKJ\\_2w](https://www.youtube.com/watch?v=uuXL5WKJ_2w)



### ZUSAMMENFASSENDE PRAXISTIPPS

- Am besten ist generelle Datensparsamkeit. Gib so wenig wie möglich von dir preis – und unter keinen Umständen sensible Daten wie Passwörter oder Kontodaten.
- Verwende für jeden Account ein eigenes starkes Passwort und aktiviere die Zwei-Faktor-Authentisierung, wo möglich.
- Prüfe E-Mails ganz genau, bevor du Anhänge oder Links öffnest.
- Lasse dich nicht zeitlich unter Druck setzen, auch wenn ein vermeintlich verlockendes Angebot nur eine kurze Zeit verfügbar sein soll.
- Frage im Zweifel deine Eltern oder eine andere Vertrauensperson. Sei immer ehrlich und suche dir Hilfe, wenn dir etwas seltsam vorkommt. So lässt sich vielleicht größerer Schaden vermeiden.



## 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](mailto: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](mailto:service-center@bsi.bund.de)

Internet: [www.bsi.bund.de](http://www.bsi.bund.de)

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

**Stand:** 09/2025

**Didaktische Aufbereitung:** Eduversum GmbH