

FÜR ELTERN

METHODEN DER CYBERKRIMINALITÄT



Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI

Liebe Eltern,

in diesem Brief stellen wir Ihnen die zweiten Lernmaterialien aus dem **Medienpaket** des BSI zur **Cybersicherheit** vor. Sie wenden sich wieder an Schülerinnen und Schüler der Klassen 5 bis 8.

Wenn Ihr Kind, wie im ersten Materialpaket empfohlen und angeleitet, sein Smartphone oder auch seinen Computer mit Maßnahmen des Basisschutzes abgesichert hat und mit Updates aktuell hält, ist es schon gut gegen die Gefahren aus dem Netz gesichert. Vor **Phishing-Versuchen** ist es damit aber leider nicht sicher. Mit Phishing-E-Mails (oder Nachrichten in anderen Diensten) versuchen Betrüger, Empfänger zur **Preisgabe von privaten Infos und Daten** zu bewegen, um diese für betrügerische Zwecke auszunutzen. Andere Nachrichten haben zum Beispiel einen Datei-Anhang oder enthalten einen Link, worüber unauffällig **Schadsoftware** eingeschleust werden soll. Täter melden sich dabei also zunächst über gängige Kommunikationskanäle, wenngleich in betrügerischer Absicht. Sie versuchen, begehrte Daten durch Täuschung, Versprechungen, Druck oder Drohung zu bekommen. Cyberkriminelle verfolgen mit Phishing verschiedene Ziele, die darauf abzielen, persönlichen oder finanziellen Schaden anzurichten. Häufige Ziele sind: Zugang zu sensiblen Daten, finanzieller Gewinn, Identitätsdiebstahl oder die Verbreitung von Schadsoftware.

Mit zunehmender Digitalisierung ist Phishing zum **Massenphänomen** geworden. Phishing steht am Anfang verschiedenartiger Delikte, die vom „einfachen“ Datendiebstahl über illegale Kontoabbuchungen bis hin zu Angriffen auf Kritische Infrastrukturen reicht. 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 sie auftreten. Das **kann jeden treffen**, auch **Kinder**. Sich zu schützen beginnt damit, das Phänomen, Merkmale und Schutzmaßnahmen zu kennen, um dauerhaft gewappnet und aufmerksam zu sein. Das lernen und erproben die Kinder in den Lernmaterialien.

Ihnen als Eltern können wir zur näheren Information zwei Podcasts und weiterführende Informationen des BSI empfehlen:

- „Update verfügbar/Ein Podcast des BSI #29: Phishing, Smishing, Quishing & Co. – Das BKA ermittelt“:
<https://www.youtube.com/watch?v=KJOTlofG4UI&list=PLUEPo9QCkRA6TIFlOIUbF8oXvqmORoq4q&index=23>
- „Update verfügbar/Ein Podcast des BSI #49: Alarmstufe Rot für private Daten – Schutz vor Identitätsdiebstahl“:
<https://www.youtube.com/watch?v=ALeJN96zEN8&t=2s>



Inhalte des Materialpakets

- **Arbeitsblatt 1** führt anschaulich mit einem Beispiel ins Thema ein und die Jugendlichen sprechen über Erfahrungen, die sie vielleicht schon mit Phishing gemacht haben.
- Auf den **Arbeitsblättern 2 und 3** werden Phishing und Schadsoftware näher erklärt und Praxistipps zum Schutz gegeben.
- **Arbeitsblatt 4** vertieft den Inhalt weiter zum Thema „Identitätsdiebstahl“.

Was Sie als Eltern konkret tun können

1. *Sprechen Sie mit Ihrem Kind grundlegend und in Ruhe über Phishing und seine Gefahren. Gehen Sie dabei auch gemeinsam die Praxistipps in den Arbeitsblättern durch.*

2. Leiten Sie Ihr Kind zur „3-Sekunden-Regel“ an: Ist mir der Absender einer Nachricht bekannt? Wirken Betreff und Inhalt klar und schlüssig? Erwarte ich diese Nachricht? Wozu Datei-Anhang oder Link? Ist Ihrem Kind etwas verdächtig, seien Sie ansprechbar und schauen Sie es sich gemeinsam an.
3. Sperren Sie Absender, die Verdächtigtes geschickt haben.
4. Vereinbaren Sie mit Ihrem Kind einen Notfallplan, wenn es doch auf ein Phishing hereingefallen ist: Sich sofort an Sie oder andere vertrauenswürdige Erwachsene wenden, und als erstes gemeinsam die betroffenen Passwörter ändern.

Noch mehr zum Thema

- 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



- 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



- 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



- 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



- Schadprogramme – Fragen & Antworten:

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



- 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

