

Arbeitsheft:

Phishing enttarnen!



Wie Betrüger*innen versuchen, an dein Passwort zu kommen und wie du das verhindern kannst.

Name: _____

Datum: _____

Abschnitt 1: Was ist Phishing?

Wie du gesehen hast, haben sich in dem Postfach deines Opas einige Mails versteckt, die Täuschungsversuche enthalten haben. Diese Art von Täuschungsversuchen nennt man auch als **Phishing**. Wenn man auf diese reinfällt, kann dies sehr gefährlich werden.

In diesem Heft wirst du lernen, was Phishing ist, wie man solche Phishing-Nachrichten erkennen und sich davor schützen kann. Doch zunächst:

1.0 – Notiere, wie viele Nachrichten du im Postfach korrekt eingeschätzt hast:

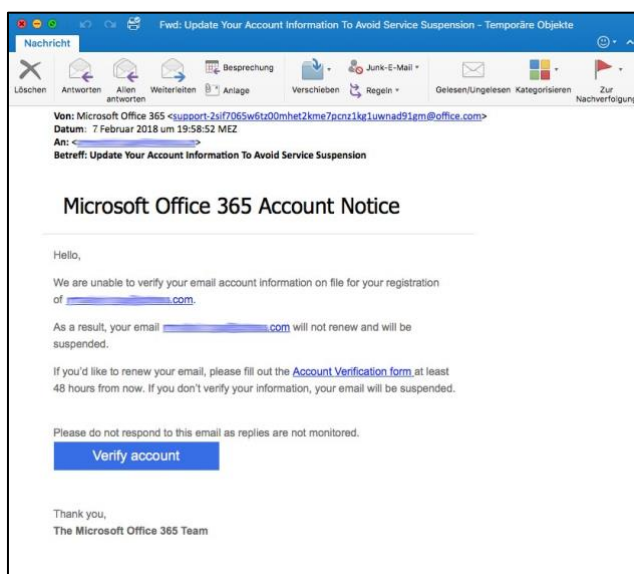
___ von ___

Was ist Phishing?

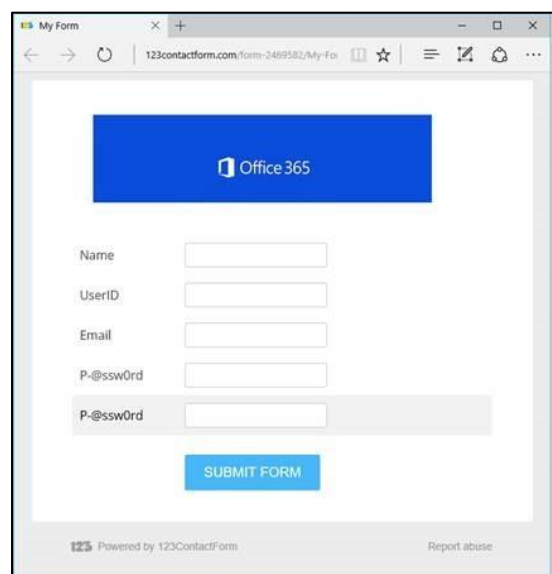
Der Begriff **Phishing** leitet sich aus den Wörtern „Passwort“ und „fishing“ (angeln) ab. Es meint so viel wie „angeln nach Passwörtern“. Es ist eine Masche von Betrüger*innen, die versuchen durch bspw. gefälschte E-Mails an persönliche und sensible Daten wie Zugangsdaten, Passwörter oder Kontodaten zu gelangen. Sie versuchen dabei die Opfer dazu zu bringen, ihre Daten selbst auf einer ebenfalls gefälschten Webseite einzugeben, um diese dann missbräuchlich zu verwenden.

Phishing ist eine Form von Cyberkriminalität. 62% der Deutschen haben schon mal wissentlich eine Phishing Nachricht erhalten.

Hier ist ein Beispiel einer E-Mail und Webseite eine Phishing-Angriffes:



Quelle: https://ap-verlag.de/clickandbuilds/WordPress/MyCMS4/wp-content/uploads/2018/02/screenshot-20180209_Retarus-PI_Office365Phishing.jpg
(letzter Zugriff: 28.08.2026)



Quelle: <https://www.msvu.ca/wp-content/uploads/2020/05/LoginExample2.jpg.jpg>
(letzter Zugriff: 28.08.2026)

1.1 – Bestimme, ob die dargestellten Aussagen *wahr* oder *falsch* sind. **Kreuze an.**

Aussage	wahr	falsch
Beim Phishing verschafft sich ein Angreifer durch Hacking Zugriff auf den Computer des Opfers.	☐	☐
Phishing ist eine seltene Form von Cyberkriminalität.	☐	☐
Eine klassische Phishing-Nachricht ist erst dann gefährlich, wenn man auf der gefälschten Webseite Daten eingibt.	☐	☐
Phisher haben es nicht nur auf Passwörter, sondern auch auf andere Zugangs- und Kontodaten abgesehen.	☐	☐
Wer niemals Passwörter per Nachricht versendet, kann kein Opfer von Phishing werden	☐	☐

Ein klassischer Phishing-Angriff folgt meistens einem bestimmten Muster:

Ablauf Phishing

1. Massenversand

Betrüger*innen versenden gefälschte E-Mail-Nachrichten an unzählige von Adressen, in der Hoffnung, dass ein Opfer darauf reinfällt.

2. Vertrauen herstellen

Mit den gefälschten E-Mails wird versucht, durch ihr Aussehen und ihre Ansprache, Vertrauen bei den Empfängern herzustellen. Darin wird das Opfer zu einer Handlung aufgefordert.

3. Weiterleitung

Die Nachricht enthält einen Link, der zu einer gefälschten Webseite führt.

4. Daten erhalten

Auf der Webseite befindet sich ein Formular, in dem die Opfer sensible Daten wie Nutzernamen, Passwörter oder Kreditkartennummern eingeben soll. Diese werden direkt an die Betrüger*innen gesendet.

5. Ausführung

Die Betrüger*innen verwenden die erhaltenen Daten für ihre (meist) kriminellen Ziele, bspw. Betrug oder Identitätsdiebstahl.

Im Folgenden sind die Schritte eines Phishing-Angriffs in einem realistischen Szenario beschrieben.

1.2 – Ordne die Schritte eines Phishing-Angriffs in die richtige Reihenfolge (1-5).

Reihenfolge	Schritt
	Ihm wird mitgeteilt, dass es eine häufige Verlosung ist, bei der schon viele Menschen gewonnen haben.
	Falk erhält eine Nachricht, dass er in einem Gewinnspiel 1.000€ gewonnen hat.
	Falk gibt seine Daten ein und überlegt sich, was er von dem Gewinn kaufen wird.
	Am nächsten Tag sieht Falk, dass ihm 2.500€ vom Konto abgebucht worden sind
	Durch einen Klick auf einen Link wird er auf eine Webseite weitergeleitet, auf der er seine persönlichen Daten und Kontodaten zur Überweisung angeben soll.

Aber es gibt eine gute Nachricht: Damit ein Phishing-Angriff funktioniert, muss das Opfer aktiv darauf reinfallen. Das kann verhindert werden, wenn man sie sicher erkennen kann.

1.3 – Erinnere dich daran, wie du das E-Mail-Postfach deines Opas bearbeitet hast. **Benenne** stichpunktartig, woran du betrügerische Nachrichten erkannt hast (min. 3).
(Hinweis: Hierfür kannst du dir gerne die Mails aus *E-Mail-Postfach.py* erneut ansehen.)

Nr.	(eigenes) Erkennungsmerkmal
1	
2	
3	

1.4 – Benenne je genanntem Erkennungsmerkmal den Betreff einer E-Mail aus dem Postfach, die dieses Merkmal aufweist.

Nr.	Betreff einer E-Mail mit (eigenem) Erkennungsmerkmal
1	
2	
3	

Viele Phishing-Nachrichten verraten sich durch typische Merkmale:

Einfache Phishing-Erkennungsmerkmale

Merkmal	Beschreibung
unpersönliche Ansprache	Da die Nachricht an möglichst viele Menschen versendet wird, werden zu Beginn allgemeine Anreden wie „Liebe/r Kunde/in“ gewählt.
ungewohnte Absender	Da die Mail von einem Betrüger kommt, hat die einen anderen Absender-Namen und E-Mail-Adresse, z.B. „gewinnspiel@gmx.de“
verdächtige Links	Auch die Links führen nicht zu Webseiten mit komischen Namen, z.B. „lotto123.ru/gewinn“
Aufforderung zur Preisgabe sensibler Daten	In der E-Mail bzw. auf der Webseite wird man aufgefordert, sensible Daten wie Passwort oder Kontonummer anzugeben.
emotionaler Druck	Um die Opfer zum Handeln zu bewegen, wird in den Nachrichten oft Druck aufgebaut: „Konto gesperrt“ oder „Gewinn abholen“
Rechtschreib- und Grammatikfehler	Häufig werden Phishing-Nachrichten aus anderen Sprachen übersetzt. Deshalb können sprachliche Fehler ein Indiz für betrügerische Nachrichten sein.

1.5 – Ordne die Merkmale den Elementen der E-Mail zu.

The screenshot shows an email titled "Konto Aktualisierung - Thunderbird". The header includes "Von: IHR PAYPAL TEAM <paypalteam@konto-aktualisierung.ru>", "An: [redacted]", and "Betreff: Konto Aktualisierung". The body text reads: "Sehr geehrte Kundin, sehr geehrter Kunde, aufgrund geänderter Nutzungsbedingungen steht eine Aktualisierung ihrer Daten aus. Diese Maßnahme ist aus Sicherheit Gründen zwingend erforderlich. Klicken sie dafür auf den unten stehenden Link und befolgen sie die notwendigen Schritte. Geben sie dabei ihre Daten vollständig und korrekt an. ACHTUNG: Wenn sie das nicht innerhalb von 24 Stunden tun, wird ihr Konto gesperrt". A link "www.konto-aktualisierung.ru/einloggen" is provided. The email ends with "Mit freundlichen Grüßen, Ihr PAYPAL TEAM".

Blue boxes and arrows identify the following elements:

- Box 1 (Subject):** Points to the subject line "Konto Aktualisierung".
- Box 2 (Sender):** Points to the sender information "IHR PAYPAL TEAM <paypalteam@konto-aktualisierung.ru>".
- Box 3 (Greeting):** Points to the salutation "Sehr geehrte Kundin, sehr geehrter Kunde,".
- Box 4 (Link):** Points to the URL "www.konto-aktualisierung.ru/einloggen".
- Box 5 (Urgency):** Points to the warning "ACHTUNG: Wenn sie das nicht innerhalb von 24 Stunden tun, wird ihr Konto gesperrt".
- Box 6 (Signature):** Points to the closing "Mit freundlichen Grüßen, Ihr PAYPAL TEAM".
- Box 7 (Toolbar):** Points to the email client's formatting toolbar.
- Box 8 (Redacted Address):** Points to the redacted recipient email address.

Du hast nun etwas über betrügerische Phishing-Nachrichten gelernt und erste Erkennungsmerkmale kennengelernt. Es ist an der Zeit dein Wissen zu testen und erneut das Postfach deines Opas aufzuräumen.

1.6 – **Bearbeite** das E-Mail-Postfach von deinem Opa erneut.

- Öffne die Anwendung „*E-Mail-Postfach.py*“.
- Siehe dir jede Mail im Postfach an und sortiere sie.
- **Bestimme**, ob du die Nachricht markieren, archivieren oder löschen möchtest.
 - Markieren: Die Nachricht ist wichtig und sollte von deinem Opa später bearbeitet bzw. beantwortet werden
 - Archivieren: Die Nachricht muss nicht direkt beantwortet werden, aber könnte später interessant sein („reine Informationen“).
 - Löschen: Die Nachricht ist unnötig/ „Spam“ und kann gelöscht werden.
- **Notiere** anschließend, wie viele Nachrichten du korrekt eingeschätzt hast:

___ von ___

Leider sind nicht alle Phishing-Nachrichten so einfach zu erkennen, wie die Nachrichten aus dem Postfach deines Opas. Phisher haben sich mit der Zeit immer ausgeklügeltere Methoden ausgedacht, um Menschen zu täuschen. Dabei können die Folgen verheerend sein.

Im weiteren Verlauf des Heftes wirst du mehr über Phishing-Angriffe erfahren und lernen, wie du auch ausgeklügeltere Phishing-Nachrichten erkennen kannst.

Abschnitt 2: Warum ist Phishing gefährlich?

Szenario

Julian hat in seinem Lieblingsspiels eine Nachricht erhalten. Darin steht, dass er ein seltenes Item gewonnen hat. Dafür müsste es sich nur kurz auf einer Seite einloggen. Er tut es und gibt sein Nutzernamen und Passwort ein. Jedoch kommt das Item nicht an. Julian denkt, dass es einfach etwas länger dauert.

Am nächsten Tag kommt er in seinen Account nicht mehr rein. Das Passwort wurde geändert. Außerdem wurden von seinem verknüpften Konto 120€ für Spielwährung abgebucht und an einem anderen Account weitergegeben. Seine Freunde sagen ihm, dass sie von Julians Account das gleiche Angebot bekommen.

Er versteht nicht, wie das passieren konnte.

2.1 – Beschreibe aus Sicht der Betrüger*innen, was Julian passiert ist. Wie sind sie vorgegangen? (**Hinweis:** Orientiere dich am typischen Ablauf eines Phishing-Angriffes)

Gefahren durch Phishing

Phishing stellt eine Form der Cyberkriminalität dar und ist eine Straftat. Die Angreifer versuchen an sensible Daten zu gelangen, um diese zu missbrauchen. Ist ein Phishing-Angriff erfolgreich, drohen dem Opfer große Schäden. Ein häufiges Verbrechen in Folge von Phishing ist **Identitätsdiebstahl**. Hier nutzen die Betrüger*innen deine Daten aus, um in deinem Namen aufzutreten, bspw. um Konten zu eröffnen oder deinen Kontakten zu schreiben. Weiter begehen die Betrüger*innen **Computerbetrug**, wenn sie die Daten verwenden, um z.B. unbefugte Einkäufe zu tätigen oder Abonnements und Verträge abzuschließen.

2.2 – Beschreibe, wie und mit welchem Ziel die Betrüger*innen Julian's Daten verwendet haben. **Erläutere**, welche Straftaten sie dabei begangen haben.

Credentials und Authentifizierungsmethoden

Wir besitzen bei verschiedenen Online-Diensten Konten. Diese enthalten häufig personenbezogene Daten von uns. Damit nicht eine beliebige Person Zugriff auf diese Daten hat, wollen Online-Dienste einen Nachweis, dass wir wirklich wir sind. Diese Nachweise heißen **Credentials**. Sie dienen der Bestätigung der Identität. Dabei nennt man die Überprüfung von Credentials **Authentifizierung**. Die häufigste Form von Credentials im Internet sind **Passwörter**.

Man kann zwischen verschiedenen **Arten von Credentials** unterscheiden, z.B.

- **Wissen** („knowledge“) – Etwas, dass die Person weiß, also im Kopf hat
- **Besitz** („ownership“) – Etwas, dass die Person physisch besitzt
- **Sein** („inherence“) – Etwas, dass die Person auszeichnet
(z.B. ein körperliches Merkmal)

2.3 – Ordne die folgenden Authentifizierungsmethoden den verschiedenen Arten von Credentials **zu**. Kreuze an.

Methode	Wissen	Besitz	Sein
Passwort	☐	☐	☐
Fingerabdruck	☐	☐	☐
Bestätigung per App ¹	☐	☐	☐
PIN der Bankkarte	☐	☐	☐
Bankkarte am Geldautomaten	☐	☐	☐

2.4 – Gebe zwei weitere Authentifizierungsmethoden an. (Falls dir keine einfallen, **recherchiere**.)

Beschreibe, was geprüft wird. **Erkläre**, welche Art von Credential es ist und warum.

Methode 1: _____

Art von Credential: _____

Methode 2: _____

Art von Credential: _____

¹ *Bestätigung per App*: Hier wird eine Benachrichtigung an ein Mobilgerät (z.B. Handy) gesendet. Auf diesem Gerät muss dann die Anmeldung bestätigt werden, z.B. „Warst du das? Ja/ Nein“

2.5 – Bestimme für die genannten Credentials, ob Phisher diese durch eine gefälschte Anmeldeseite erlangen werden können, um dauerhaften Zugriff auf das Konto zu erhalten. **Begründe** deine Einschätzung stichpunktartig.

Credential	Kann erlangt werden (ja/nein)	Warum (nicht)?
Passwort		
Bankkarte		
Bestätigung per App		
PIN der Bankkarte		

2.6 – Vergleiche Credentials des Wissens mit Credentials des Besitzes. Sind diese leicht oder schwer durch Phisher zu erlangen?

Credential-Art	Erklärung
Wissen	
Besitz	

2.7 – Inwieweit ist es gefährlich, für verschiedene Konten das gleiche Credential zu verwenden? **Vergleiche** Credentials des Wissens mit Credentials des Besitzes.

Credential-Art	Erklärung
Wissen	
Besitz	

2.8 – Recherchiere den Begriff „Zwei-Faktor-Authentifizierung“ (2FA).

Beschreibe, was dieses Verfahren auszeichnet. Verwende den Begriff *Credential*.

2.9 – Erkläre warum diese Art der Authentifizierung in Bezug auf Phishing für mehr Sicherheit sorgt.

2.10 – Erkläre worauf bei der Einrichtung von 2FA geachtet werden sollte, um besonders effektiv gegen Phishing zu sein.

Abschnitt 3: Warum funktioniert Phishing?

Jetzt stellt sich aber eine wichtige Frage: Wenn das Phänomen Phishing und deren Gefahren bekannt sind, warum fallen dann immer noch Menschen auf diese Art des Cyber-Angriffs rein?

3.1 – Notiere eine kurze, **begründete** Vermutung.

Social Engineering

Bei Cyberangriffen wird sich unerlaubt Zugriff auf Computersysteme verschafft. Klassischerweise werden hier bspw. Sicherheitslücken in der Software ausgenutzt. Jedoch sind Systeme heutzutage häufig gut geschützt, was technische Angriffe erschwert. Aus diesem Grund greifen Phishing-Betrüger*innen nicht die Technik, sondern den Menschen an.

Hierfür wird sog. **Social Engineering** angewendet. Das beschreibt zwischenmenschliches Beeinflussen mit dem Ziel, bei Personen ein bestimmtes Verhalten hervorzurufen. Das machen sie, indem sie z.B. Druck auf die Opfer ausüben. Ziel ist es, die zu unüberlegten Handlungen zu bewegen.

3.2 – Beschreibe, mit welchem konkreten Ziel *Social Engineering* bei Phishing-Angriffen eingesetzt wird. Zu welcher Handlung sollen die Opfer bewegt werden?

3.3 – Bestimme, bei welchen der Angriffe es sich um Social Engineering handelt.

Angriff	Social Engineering? (ja/ nein)
Eine gefälschte Gewinn-Nachricht sagt, man solle seine Zugangsdaten angeben.	
Ein Hacker nutzt eine Sicherheitslücke im Server einer Firma aus.	
Ein Programm probiert automatisch viele Passwörter aus.	
Ein Anrufer gibt sich als IT-Support aus und fragt nach dem Passwort.	

3.4 – Erkläre, warum Phishing eine besondere Form des Cyberangriffes darstellt. Inwiefern unterscheidet es sich von anderen Formen von Cyberangriffen?

Hinweis

Seriöse Unternehmen fordern ihre Kunden niemals per E-Mail zur Eingabe vertraulicher Informationen auf.

Fassen wir nun zusammen, was wir über Phishing als Cyber-Angriff gelernt haben.

3.5 – Formuliere eine zusammenfassende **Definition** für den Begriff **Phishing**. Verwende dabei die Begriffe *Cyber-Angriff*, *Credentials* und *Social Engineering*.

Phishing

Kommen wir nun nochmal zurück zum Fall von Julian:

Szenario

Julian konnte den Betrug bei der Spieleplattform melden und hat seinen Account wiederbekommen. Seitdem ist er sehr vorsichtig und versucht auch, seine Freunde zu warnen. Seinen Kumpel Mats konnte er nicht überzeugen. Als er ihm von dem Vorfall berichtet, sagt er nur:

„Man muss auch nicht zu vorsichtig sein. Ja, in deinem Fall ist es blöd gelaufen, aber du hast deinen Account ja wieder. Aber wenn die Nachricht echt gewesen wäre, wäre das echt cool. Die Chance will man doch nicht verpassen!“

3.6 – Schreibe eine kurze Antwort aus der Perspektive von Julian. **Begründe**, warum Mats Einstellung potenziell gefährlich und Datensicherheit wichtig ist.

Abschnitt 4: Die Methoden der Phisher

Viele Betrüger*innen geben sich große Mühe, dass ihre Phishing-Angriffe nicht direkt als Täuschung erkannt werden. Dafür benutzen sie eine Reihe an Tricks, um die Nachrichten und Webseiten möglichst echt aussehen zu lassen.

Aber keine Sorge! Wenn man diese Tricks kennt und weiß, worauf man achten muss, lassen sich viele Phishing-Angriffe gut erkennen.

In diesem Abschnitt lernst du, welche Tricks die Betrüger*innen verwenden und wie du ihre Nachrichten und Webseiten trotzdem enttarnen kannst.

Im weiteren Verlauf des Heftes gibt es mehrere, unterschiedliche Module. Jedes behandelt einen anderen Aspekt von Phishing. Dabei sind diese unterschiedlich lang und in verschiedene Bereiche gegliedert.

4.1 – Bearbeite Module zur Erkennung von Phishing deiner Wahl. Dabei sollst du mindestens folgende Anzahl Module abschließen:

- Mind. 2 Module aus dem Bereich „Warnzeichen“
- Mind. 1 Modul aus dem Bereich „Technische Aspekte“
- Mind. 2 Module aus dem Bereich „Vertiefung“

Kategorie	Modul	erledigt
Warnzeichen	look and feel	☐
	Absenderadresse	☐
	Versteckte Links	☐
	Domain-Spoofing 1*	☐
Technische Aspekte	Netzwerkübertragung und Zertifikate	☐
	Domain-Spoofing 2*	☐
Vertiefung	Psychologische Vertiefung	☐
	Spear-Phishing	☐
	Schadsoftware	☐
	Phishing in der Politik	☐

*Domain-Spoofing 2 stellt eine erweiterte Version von Domain-Spoofing 1 dar. Bearbeite nur eines dieser Module!

Hake nach jeder Bearbeitung das entsprechende Modul in der Tabelle ab.

Wenn du fertig bist, geht das Arbeitsheft auf der nächsten Seite weiter!

Abschnitt 5: Phishing entlarven

Sehr gut! Du hast nun eine Reihe an Tricks von Phishing-Betrüger*innen kennengelernt. Nun hast du das Werkzeug zu einem*r richtigen Phishing-Detektiv*in.

Lass uns dein neues Wissen direkt testen:

5.1 – Bearbeite das E-Mail-Postfach von deinem Opa erneut.

- Öffne die Anwendung „*E-Mail-Postfach.py*“.
- Siehe dir jede Mail im Postfach an und sortiere sie.
- **Bestimme**, ob du die Nachricht markieren, archivieren oder löschen möchtest.
 - Markieren: Die Nachricht ist wichtig und sollte von deinem Opa später bearbeitet bzw. beantwortet werden
 - Archivieren: Die Nachricht muss nicht direkt beantwortet werden, aber könnte später interessant sein („reine Informationen“).
 - Löschen: Die Nachricht ist unnötig/ „Spam“ und kann gelöscht werden.
- **Notiere** anschließend, wie viele Nachrichten du korrekt eingeschätzt hast:

__ __ __ von __ __ __

5.2 – Vergleiche die Anzahl der richtig eingeordneten Nachrichten aus deinen vorherigen Versuchen. **Beschreibe**, ob du eine Veränderung festgestellt hast.

Versuch 1:		Versuch 2:		Versuch 3:	
-------------------	--	-------------------	--	-------------------	--

5.3 – Betrachte deine Stichpunkte zur intuitiven Erkennung von Phishing aus **1.3**.

Ordne deine Stichpunkte mit deinem neuen Wissen **ein**.

Begründe (fachsprachlich), ob es sich um geeignete Strategien zur Erkennung von Phishing handelt.

Achtung

Wenn man auf diese Merkmale achtet, hat man gute Voraussetzungen, sich vor vielen Phishing-Angriffen zu schützen. Dennoch entwickeln sich die Methoden der Betrüger*innen immer weiter. Bleibe daher weiterhin vorsichtig, wenn dir eine Nachricht komisch vorkommt, auch wenn du keine bekannten Merkmale feststellst.

Nicht immer sind die Merkmale offensichtlich. Manchmal ist man sich auch nach umfangreicher Prüfung nicht sicher, ob es sich um eine seriöse oder betrügerische Nachricht handelt.

An das Unternehmen/ die Person wenden

Digitale Kommunikation birgt viele potenzielle Gefahren. Manchmal ist die sicherste Möglichkeit bei Unsicherheit, die Nachricht nicht zu beantworten und sich direkt an die „vermeintlichen“ Absender auf einen analogen Weg zu wenden – selbst wenn es dringend ist.

5.4 – Beschreibe mögliche konkrete Handlungen, die man tun kann, wenn man nicht sicher ist, ob es sich um eine seriöse Nachricht handelt.

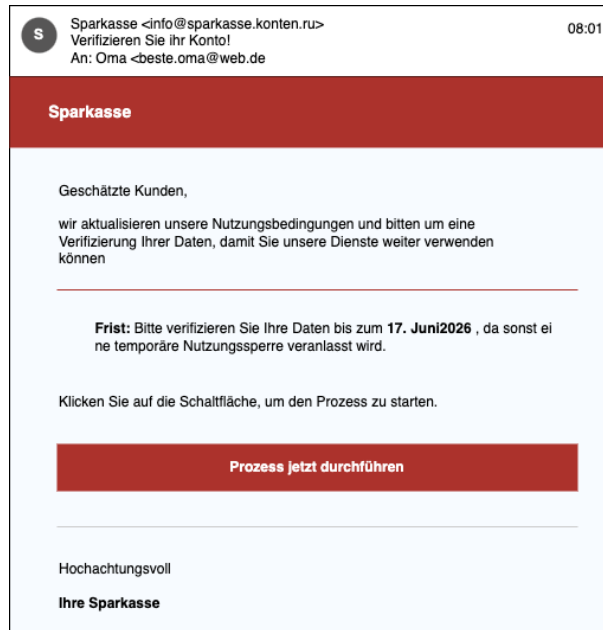
5.4 – Erläutere, warum es bei den von dir beschriebenen Handlungen um eine geeignete Strategie im Umgang mit Phishing handelt.

Abschnitt 6: Anti-Phishing-Checkliste

Szenario

Deine Oma hat eine Nachricht von ihrer Bank erhalten mit der Aufforderung, ihr Online-Konto erneut zu verifizieren. Da sie nicht weiß, was das bedeutet, bittet sie dich das zu machen. Als du die Nachricht siehst, bemerkst du sofort, dass es Phishing ist.

Als du deine Oma darauf ansprichst, sagt sie nur: „Aber meine Bank schreibt mir doch öfter. Das sieht aus wie immer. Woher soll ich das wissen?“



6.1 – Nenne mindeste 3 Merkmale, an denen deine Oma erkannt haben könnte, dass es sich bei der Nachricht um einen Phishing-Angriff handelt.

6.2 – Beschreibe, wie deine Oma und du jeweils auf die Nachricht reagieren. Überlege, was die unterschiedliche Beschreibung verursacht.

Wir haben zuletzt viel über verschiedene Methoden und Tricks von Phishing-Angreifern erfahren und gelernt, wie man diese erkennen kann.

Erinnere dich an **Abschnitt 2** zurück. Dort hast du erfahren, dass Phishing eine besondere Form von Cyberangriff ist. Dabei wurde behauptet, dass der Erfolg eines Phishing-Angriffs auch von dem Wissen der Zielpersonen abhängt.

6.3 – Erkläre in eigenen Worten, warum die Unwissenheit des Opfers zum Erfolg von Phishing-Angriffen beiträgt.

Um die Gefahr von Phishing-Angriffen zu verringern, spielt Aufklärung eine zentrale Rolle. Um sie sicher zu erkennen, benötigt man drei Arten von Wissen:

- **Wissen, dass es Phishing überhaupt gibt**

Wer die Gefahren und Methoden von Internetbetrüger*innen nicht kennt, ist auch weniger achtsam.

- **Grundwissen über Computersysteme**

z.B. wie Domains und E-Mails aufgebaut sind. Nur damit lassen sich echte und gefälschte Absender auseinanderhalten.

- **Grundwissen über Sicherheitsindikatoren**

Damit sind typische Anzeichen für Echtheit gemeint. Dazu gehört z.B., dass Unternehmen nie sensible Daten per E-Mail abfragen oder „https“ eine verschlüsselte Verbindung anzeigt.

Da wir nun bereits einiges über Phishing sowie die dahinterliegenden Methoden und Gefahren wissen, werden wir nun zum Schutz davor beitragen. Dazu gestalten wir zum Abschluss einen aufklärenden Flyer:

6.4 – Gestaltet eine Anti-Phishing-Checklist als Flyer.

Der Flyer soll 3 Aspekte beinhalten:

1. **Erklärt**, bei welcher Art von Nachrichten man besonders vorsichtig sein sollte und warum.
2. **Erklärt** Maßnahmen, mit denen man überprüfen kann, ob es sich um eine Phishing Nachricht handelt. Je Maßnahme soll ...
 - a. eine ansprechende Überschrift gewählt werden.
 - b. die Maßnahme kurz **beschrieben** werden.
 - c. **begründet** werden, warum diese Maßnahme „wirksam“ ist.
(Wählt die für euch 5 hilfreichsten Maßnahmen aus.)
3. **Erklärt**, was man tun kann, wenn man sich nicht sicher ist.

Der Flyer ist für Personen, die sich nicht mit Phishing auseinandergesetzt haben. Daher sollten die Maßnahmen sowie deren Begründungen möglichst verständlich sein.

Diese Aufgabe soll als **Gruppe** bearbeitet werden. Such dir **bis zu 2 weitere Mitschüler*innen**, die genauso weit in der Bearbeitung des Arbeitsheftes sind wie du. Diskutiert gemeinsam mögliche Antworten und klärt euch gegenseitig auf, falls ihr nicht die gleichen Module bearbeitet habt.

(Wenn du noch etwas Zeit überbrücken musst, kannst du bereits mit der Planung des Flyers beginnen oder weitere kurze Module bearbeiten.)

Verwendet zur Gestaltung des Flyers die **Vorlage auf der nächsten Seite**.

Anti-Phishing-Checkliste

Bei dieser Art von Nachricht sollte ich vorsichtig sein:

So kann ich überprüfen, ob eine verdächtige Nachricht tatsächlich Phishing ist:

Nr.	Maßnahme	Beschreibung	Begründung
1			
2			
3			
4			
5			

Was kann ich tun, wenn ich mir dennoch unsicher bin?
