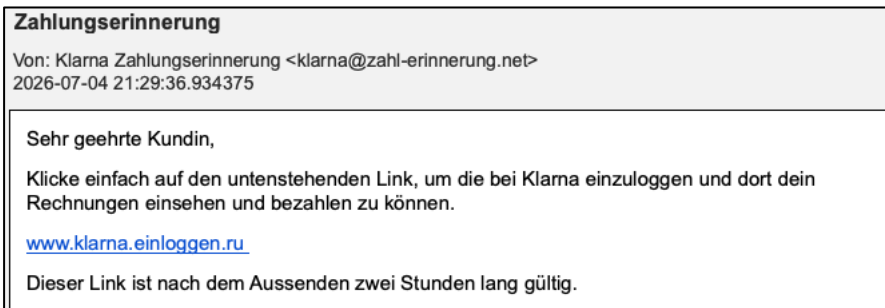


Technische Aspekte 2: Domain-Spoofing

Diese Mail ist eine Phishing-Nachricht aus dem Postfach deines Opas:

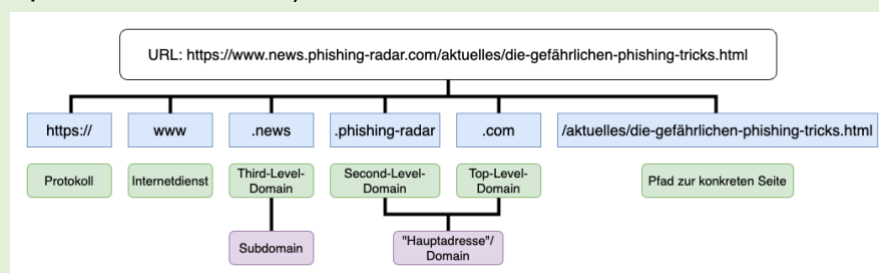


A.1 – Warum ist diese Nachricht verdächtig? Notiere eine Vermutung.

Diese Nachricht wurde von einer E-Mail gesendet, die auf den ersten Blick plausibel aussieht. Auch der darin enthaltene Link ergibt zunächst Sinn. Doch bei genauerem Hinsehen, fällt etwas auf. Die URL www.klarna.einloggen.ru zeigt auf eine russische Webseite, obwohl Klarna ein schwedisches Unternehmen ist. Um dies zu verstehen, benötigen wir zunächst etwas Wissen über Domains und URLs.

Hintergrund: Domains und URLs

Eine Domain bezeichnet den menschenlesbaren Namen eines Servers. Sie ist eindeutig, d.h. jeder Name kann nur einmal vergeben werden. Eine URL (Uniform Resource Locator) ist eine eindeutige Adresse, die auf eine konkrete Ressource im Internet (bspw. eine Webseite) verweist. Sie hat eine feste Struktur:



Third-Level-Domain	Nähere Strukturierung des Servers	Top-Level-Domain	Länder-/Organisationscode
Second-Level-Domain	Name des Anbieters/ Servers	Pfad	Verweis auf konkrete Webseite

Die eigentümerbestimmende Domain liest man rechts vom ersten „/“ bis zur Second-Level-Domain. Alles darüber hinaus ist die Subdomain und frei wählbar.

Auch E-Mail-Adressen besitzen eine Domain:

benutzername@domain

Für mehr Informationen, schaue hier: http://www.paul-orzessek.de/grundkurs_internet/internetadresse.htm

A.2 – Bestimme für jede URL die Hauptadresse.

Webseite	Hauptadresse
www.planetarium.berlin/zeiss-grossplanetarium/geschichte	
www.dfb.fanshop.io/login	
www.sparkasse.de.suport.ru/verifizieren	

A.3 – Recherchiere nach dem Unternehmen Klarna. **Gebe** die Hauptadresse **an**.

A.4 – Beschreibe wie sich die URL aus der Mail von der Klarna-Domain unterscheidet.

Domain-Spoofing

Domain-Spoofing beschreibt eine Art der Täuschung, bei der Betrüger*innen versuchen, die Domain eines seriösen Unternehmens zu imitieren. Hierfür gibt es zwei typische Angriffspunkte:

- **URL-Spoofing**

Hier wird die URL ähnlich zu einer seriösen Webseite benannt. Dies kann durch ähnliche Zeichen (z.B. „l“ und „1“) oder Schreibweisen passieren. Auch kann der seriöse Name als Teil der Second- oder Third-Level-Domain verwendet werden.

beispielbank.de sicher-beispielbank.com beispielbank.de.konto.net

- **E-Mail-Spoofing**

Hier wird die E-Mail eines seriösen Unternehmens nachgeahmt. Auch dies kann durch ähnliche Zeichen (z.B. „l“ und „1“) oder Schreibweisen passieren. Dazu kann der seriöse Name im Benutzernamen, als Teil der Second- oder der Third-Level-Domain verwendet werden.

beispielbank@kontakt.io kontakt@beispielbank.konto.net

A.5 – Bestimme, ob du den gegebenen E-Mails/URLs vertrauen kannst.
 Falls nein, **gebe an**, welche E-Mails/URLs vermutlich nachgeahmt werden sollten.

E-Mail/ URL	Vertrauen? (ja/ nein)	Original
info@google.com.ru		
no-reply@email.apple.com		
www.youtoobe-login.co		
www.paypal.com		
www.instagram.com		

A.6 – Erkläre, warum Betrüger*innen die Strategie „Domain-Spoofing“ verwenden.
 Welches Ziel verfolgen sie und warum soll es erfolgsversprechend sein?

Viele Domain-Spoofing-Versuche kann man bei genauerer Betrachtung und mit Wissen über den Aufbau von Domains erkennen. Jedoch sind nicht alle so einfach zu durchschauen. Betrachten wir folgendes Beispiel:

a) google.com	b) google.com
---------------	---------------

A.7 – Fällt dir zwischen den Domains a) und b) ein Unterschied auf? **Beschreibe** deinen Eindruck.

Obwohl die beiden Domains auf den ersten Blick identisch aussehen, handelt es sich um unterschiedliche Texte. Doch wie kann das sein? Um dies zu verstehen, müssen wir die Darstellung von Zeichen im Computer genauer betrachten.

Hintergrund: Zeichendarstellung im Computer

Vielleicht hast du schonmal gehört, dass ein Computer nur aus „Einsen und Nullen“ besteht. Er arbeitet mit nur mit Zahlen, die er im binären System als 1 für „an“ oder 0 für „aus“ speichert. Aus diesem Grund kennt er keine Buchstaben. Um trotzdem Wörter und Sätze darstellen zu können, bedient man sich einen Trick:

Man legt ein festes Zahlensystem fest, bei dem jeder Buchstabe und jedes Zeichen eine feste Zahl bekommt. Ein bekanntes System hierfür ist ASCII. Dadurch, dass jedes Zeichen einer eindeutigen Zahl zugeordnet wird, lassen sich Texte einheitlich darstellen und austauschen.

ASCII-Code (Ausschnitt)					
A	65	J	74	S	83
B	66	K	75	T	84
C	67	L	76	U	85
D	68	M	77	V	86
E	69	N	78	W	87
F	70	O	79	X	88
G	71	P	80	Y	89
H	72	Q	81	Z	90
I	73	R	82	Leerzeichen	32

A.8 – Gebe deinen Vornamen im ASCII-Code **an**. (Benutze nur Großbuchstaben)

Hier ist eine erweiterte ASCII-Liste mit allen Zeichen und den entsprechenden Zahlen.

<https://www.ibm.com/docs/de/aix/7.3.0?topic=adapters-ascii-decimal-hexadecimal-octal-binary-conversion-table>

(Hinweis: Wie angedeutet kann man Zahlen in verschiedenen Zahlensystemen darstellen. Unser „alltägliches“ Zahlensystem heißt Dezimal- oder auch Zehnersystem. Das liegt daran, dass wir zehn Ziffern, nämlich 0 bis 9, verwenden.)

A.9 – Bestimme das im ASCII-Code dargestellte Wort, indem du den Zahlen das entsprechende Zeichen zuordnest.

80 97 115 115 119 111 114 116

Hintergrund: erweiterte Zeichendarstellung

Der ASCII-Code zur Darstellung von Zeichen ist im 7-Bit-System entwickelt worden. Aus diesem Grund besitzt er eine natürliche Grenze von 128 verschiedenen Zeichen. Während das ausreicht, um europäische Sprachen mit lateinischen Buchstaben darzustellen, sind dies nicht genug, um weitere Sprachen wie Russisch, Chinesisch oder Arabisch, die andere Zeichen verwenden, abzubilden.

Aus diesem wurde ein weiteres System entwickelt, um mehr Zeichen zu berücksichtigen: der Unicode-Standard. Dieser umfasst weit mehr Zeichen und kann bspw. kyrillische Buchstaben, Symbole und Emojis abbilden.

Neben den gezeigten Tabellen zur Umwandlung von Zahlen in Zeichen gibt es auch Converter-Programme, die dies automatisch tun:

<https://www.webtoolpanel.com/de/developer-tools/ascii-converter>

(Achtung: Da ASCII umgangssprachlich bekannter ist und die ASCII-Codes im Unicode übereinstimmen, werden solche Umwandlungsprogramme häufig fälschlicherweise „ASCII-Converter“ genannt. Dabei deckt dieses Programm alle Zeichen des Unicode ab.)

A.10 – Bestimme wie der Satz im Unicode dargestellt wird.

Nein heißt Her

Auch wenn dieses erweiterte Zeichensystem eine inklusive und internationale Form der digitalen Kommunikation ermöglicht, kann es zugleich für Phishing missbraucht werden. Kommen wir zurück zu unserem Beispiel der Domains a) und b):

A.11 – Lasse dir die Domains a) und b) durch den Converter in Zahlen umwandeln und vergleiche diese miteinander. **Beschreibe** deine Beobachtung.

Hinweis: Öffne das Begleitmaterial *T2_Domainspoofing*, um den Text zu kopieren.

A.12 – Setze deine Beobachtung mit Domain-Spoofing **in Beziehung**. Sind beide Domains vertrauenswürdig?

Homographen-Angriffe

Diese fortgeschrittene Variante von Domain-Spoofing nennt man auch Homographen-Angriffe. Sie machen sich für Täuschung sogenannte Homoglyphen (griech. *homós* = „gleich“) zunutze, also Zeichen, die wie andere Unicode-Zeichen aussehen. Hierzu werden bspw. kyrillische Buchstaben verwendet. So sollen Domains nachgeahmt werden, ohne dass diese visuell erkannt werden kann.

A.13 – Erkläre folgende Aussage.

„Domain-Spoofing kann man nicht immer mit dem bloßen Auge erkennen!“

A.14 – Bestimme, ob du den gegebenen E-Mails/URLs vertrauen kannst.

Falls nein, **begründe**.

Hinweis: Öffne das Begleitmaterial *T2_Domainspoofing*, um die URLs zu kopieren.

URLs	Vertrauen? (ja/ nein)	Begründung
paypal.com		
google.com		
arnazon.de		
ebay.com		

Maßnahme

A.15 – Erkläre, inwieweit dir dieses Modul bei der Erkennung von Phishing geholfen hat. Worauf sollte man bei der Beurteilung von E-Mails bzw. Webseiten achten und warum?
