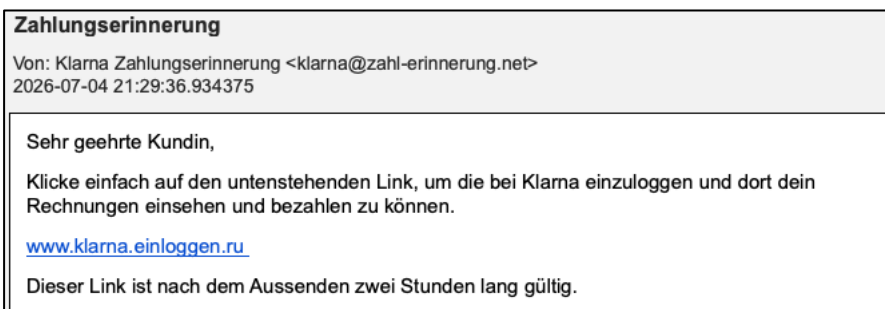


Warnzeichen 4: Domain-Spoofing

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

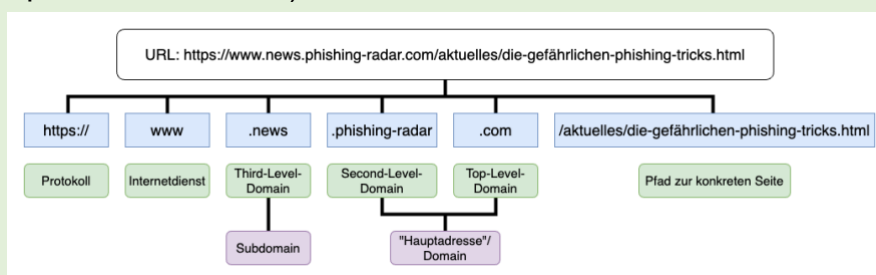


A.1 – Warum ist diese Nachricht verdächtig? Notiere eine Vermutung.

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?

Maßnahme

A.7 – 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?
