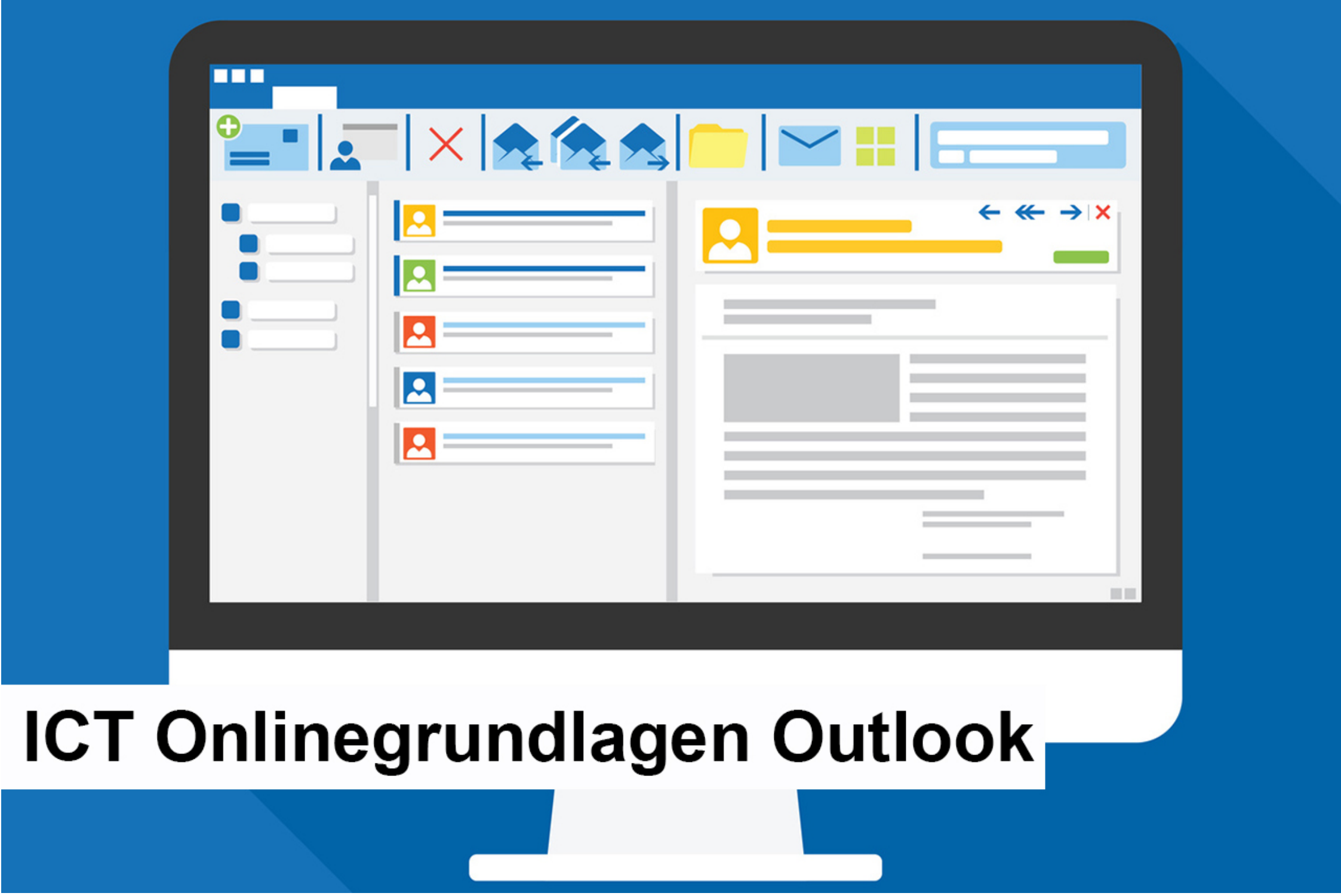


ICT Onlinegrundlagen Outlook

Online- Grundlagen

Outlook 2016

Inhalt

Erklärung der Symbole

In den Arbeitsaufträgen kommen folgende Symbole vor:

	Bei diesem Symbol ist ein schriftlicher Arbeitsauftrag verlangt.
	Hier sollst du überwiegend am Computer arbeiten. Alle Dateien, die du benötigst findest du im Ordner **Modul 7**.
	Bist du zügig unterwegs? Dann versuche doch mal die Zusatzaufgaben zu bearbeiten.
	Kannst du dich an den Inhalt der vorherigen Themen erinnern? Mit den Repetitionsaufgaben kannst du dein Wissen auffrischen.

6. Gefahren durch E-Mails

Meine Lernziele

- ☐ Ich bin mir der Gefahr bewusst, dass man unerwünschte, betrügerische E-Mails erhalten kann (4.3.5).
- ☐ Ich weiss, was mit Phishing bezweckt wird (4.3.6).
- ☐ Ich bin mir der Gefahr bewusst, dass der Computer mit einem Virus infiziert durch Öffnen einer unerwünschten E-Mail eines Attachments werden kann (7.5.2.3).
- ☐ Ich verstehe, was eine digitale Signatur ist (7.5.2.4).

So wie es Risiken im alltäglichen Leben gibt, findet man auch diese im World Wide Web. Jede Person, die eine E-Mail-Adresse besitzt, muss sich der Gefahr bewusst sein, dass man betrügerische und unerwünschte E-Mails erhalten kann.

Phishing und betrügerische E-Mails

Die Gefahr des **Phishings** ist im Internet allgegenwärtig. Der Benutzer bekommt eine gefälschte E-Mail mit einem scheinbar bekannten Absender beispielsweise von der eigenen Bank oder einem anderen Unternehmen (Apple, Swisscom, Migros, …). In der Nachricht erhält man die Aufforderung, entweder die Personalien und das Passwort zu bestätigen, einen gesendeten Link anzuklicken (siehe Abbildung) oder einen E-Mail-Anhang zu öffnen.

Durch das Anklicken eines Links, wird man auf eine gefälschte Webseite weitergeleitet, auf der Daten wie Benutzernamen, Kreditkartennummern oder Passwörter eingegeben werden sollen. Die gefälschte Webseite sieht wie die echte Internetseite aus, jedoch wird in der Adresszeile eine andere URL angezeigt.

Diese Art von E-Mails sollten gelöscht werden und man sollte niemals darauf reagieren. Weder eine Bank noch ein anderes Unternehmen wird Kunden per E-Mail kontaktieren, um persönliche Daten anzufragen. Man erkennt eine Phishing Mail an einer unbekannten URL, am unbekannten Absender und häufig am schlechten Deutsch.

Viren können sich nicht selbst vermehren, sondern brauchen dazu ein Programm oder eine Datei (wird Wirt genannt). Erhält man eine E-Mail mit einem virenverseuchten Anhang (Attachment), so wird der Virus erst aktiv, wenn der Anhang geöffnet wird.
Besteht der Verdacht, dass eine E-Mail einen Virus enthält, so sollte diese sofort gelöscht werden.

Spam und Hoaxes

Gelegentlich kann es auch vorkommen, dass unerwünschte E-Mails, wie **SPAMs** im Posteingang empfangen werden. SPAMs sind zwar lästig, jedoch eher harmlos. SPAMs beinhalten meistens unerwünschte Werbung. Häufig findet man bei diesen E-Mails einen Link, mit welchem man scheinbar den Spam abbestellen kann. Das funktioniert leider häufig nicht und man sollte diesen Link nicht anklicken, da der Verteiler erkennt, dass diese E-Mailadresse existiert und korrekt ist.

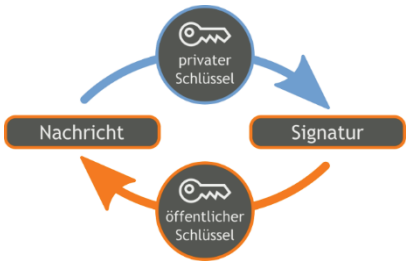
Lästig sind dagegen die verschickten Falschnachrichten (**Hoaxes**), die als Kettenbriefe verschickt werden. Auf diese Nachrichten solltest du auf keinen Fall reagieren. Häufig wird eine vertrauenserweckende Quelle, wie Microsoft, die Polizei oder der Kanton im Text genannt und meistens ist von „gestern“ die Rede, ohne dass ein Datum angegeben wird. Es wird auf vertrauenswürdige Quellen verwiesen, ohne dass diese angegeben werden. Diese Nachrichten fordern auf, dass sie so schnell wie möglich an alle Bekannte weitergeleitet werden sollen. Wie schon geschrieben – bitte sofort löschen.

Digitale Signatur

Digitale Signaturen spielen beim elektronischen Nachrichtenaustausch eine ähnliche Rolle wie Unterschriften auf Papierdokumenten. Eine digitale Signatur wird benutzt, um die Integrität, Authentizität und Verbindlichkeit zu gewährleisten.

Integrität:	Die erhaltene Nachricht wurde von keiner dritten Person manipuliert.
Authentizität:	Die erhaltene Nachricht stammt wirklich von der Person, die als Absender angegeben ist.
Verbindlichkeit:	Der Absender der Nachricht kann nicht abstreiten, die Nachricht verfasst zu haben.

Die Identifizierung ist besonders bei sensiblen Inhalten einer E-Mail oder bei Online-Einkäufen wichtig.



Die Technik der digitalen Signatur beruht auf zwei elektronischen Schlüsseln, einem öffentlichen und einem privaten Schlüssel.

Inhalte, die mit dem privaten Schlüssel verschlüsselt werden, können nur mit dem öffentlichen Schlüssel entschlüsselt werden (siehe Abbildung). Der private Schlüssel bleibt immer geheim, der öffentliche ist jedermann zugänglich. Der private Schlüssel kann durch den öffentlichen Schlüssel nicht berechnet werden.

Für das Erzeugen einer digitalen Signatur kann einer Person ein einmaliger geheimer privater Signaturschlüssel eindeutig zugeordnet werden. Dieser private Schlüssel befindet sich auf einer Chipkarte und kann nur zusammen mit einer PIN-Nummer verwendet werden. Damit kann der Inhaber des Schlüssels immer wieder Dokumente signieren. Mit einem öffentlichen Schlüssel kann die Signatur jederzeit überprüft werden.

Aufgaben:

1. Wie können Viren auf einen Computer gelangen?

_____

2. Verbinde den Begriff mit der entsprechenden Aussage.

PHARMING	⊙	⊙	Der Benutzer wird auf eine gefälschte Webseite umgeleitet, obwohl die Adresse richtig eingegeben wurde.
SPAM	⊙	⊙	… ist die Beschaffung persönlicher Daten anderer Personen mit gefälschten E-Mails.
HOAX	⊙	⊙	… sind unerwünschte Nachrichten, die massenhaft versendet werden. Sie beinhalten meist Werbung.
Phishing	⊙	⊙	… sind Kettenbriefe mit Falschmeldungen.

3. Schaue dir den Videoclip **6_Hoax.mp4** an.
   a. Zähle ein Beispiel für Hoax auf.

_____

   b. Woran lasst sich ein Hoax erkennen?

_____

_____

_____

4. Erläutere, was eine Phishing-Angriff ist.

_____

5. Woran kannst du einen Phishing-Versuch erkennen?

_____

_____

_____

6. Was ist eine digitale Signatur?

_____

_____

7. Streiche den falschen Begriff durch, so dass eine richtige Aussage entsteht.

- Mit einem **privaten/ öffentlichen** Schlüssel wird die digitale Signatur erzeugt.
- Mit dem **privaten/ öffentlichen** Schlüssel wird die Authentizität der Unterschrift überprüft.
- **Authentizität/ Integrität** bedeutet, dass eine Nachricht eindeutig dem Absender zugeordnet werden kann.
- **Authentizität/ Integrität** bedeutet, dass der Inhalt einer Nachricht unverfälscht ist.
- **Verbindlichkeit/ Integrität:** Der Absender ist tatsächlich der Verfasser der Nachricht und kann dies auch nicht abstreiten.

8. Tom hat eine Phishing-Mail mit einer Mahnung von der *Inkasso Online Pay AG* erhalten. Diese Zahlungsaufforderung ist gefälscht.
   a. Schaue dir den Videoclip **6_InkassoOnlinePayAG** an.
   b. Wie kann Tom nun richtig auf diese Phishing-Mail reagieren?

   _____

   _____

   _____

9. Schaue im Internet nach, woher der Name SPAM kommt.

   _____

   _____

10. Aus welchen Begriffen setzt sich das Wort Phishing zusammen? Du kannst danach googlen.

    _____

    _____

Gefahren durch E-Mails

Kapitel 6

1. Wie können Viren auf einen Computer gelangen?

- Öffnen einer unerwünschten E-Mail oder eines Attachments
- Speichermedien, wie Speicherkarten und USB- Sticks
- Surfen auf unseriösen Internetseiten
- Herunterladen von Dateien aus dem Internet
- Illegale Software- und Musiktauschbörsen

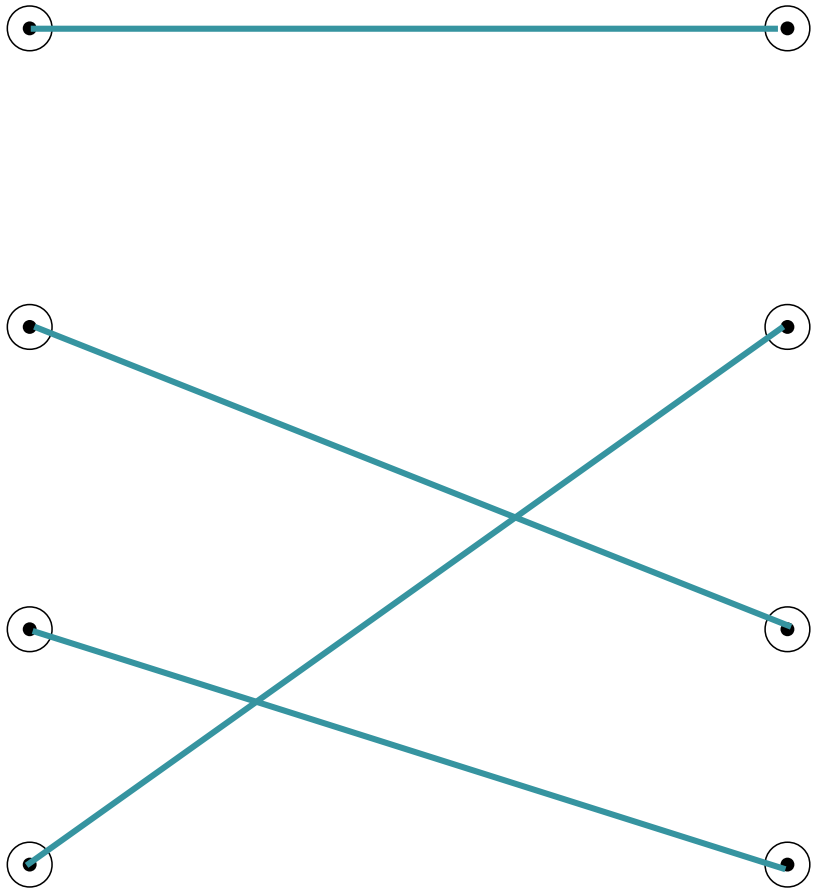
2. Verbinde den Begriff mit der entsprechenden Aussage.

PHARMING

SPAM

HOAX

Phishing



Der Benutzer wird auf eine gefälschte Webseite umgeleitet, obwohl die Adresse richtig eingegeben wurde.

… ist die Beschaffung persönlicher Daten anderer Personen mit gefälschten E-Mails.

… sind unerwünschte Nachrichten, die massenhaft versendet werden. Sie beinhalten meist Werbung.

… sind Kettenbriefe mit Falschmeldungen.

3a. Zähle ein Beispiel für Hoax auf.

- Drohung
- Falscher Aufruf
- Protestieren, Unterschrift abgeben
- Tränendrüsen-Nachricht

Beispiele:

- Dieses Baby hat Krebs, Facebook zahlt für jedes Bild… wenn du ein Herz hast teile das Foto.
- Wichtige Meldung zum 10 Jährigen Geburtstag von WhatsApp: Deine geliebte App kostet ab Montag 25€ pro Monat, ausser du leitest diese Nachricht weiter.

3b. Woran lasst sich ein Hoax erkennen?

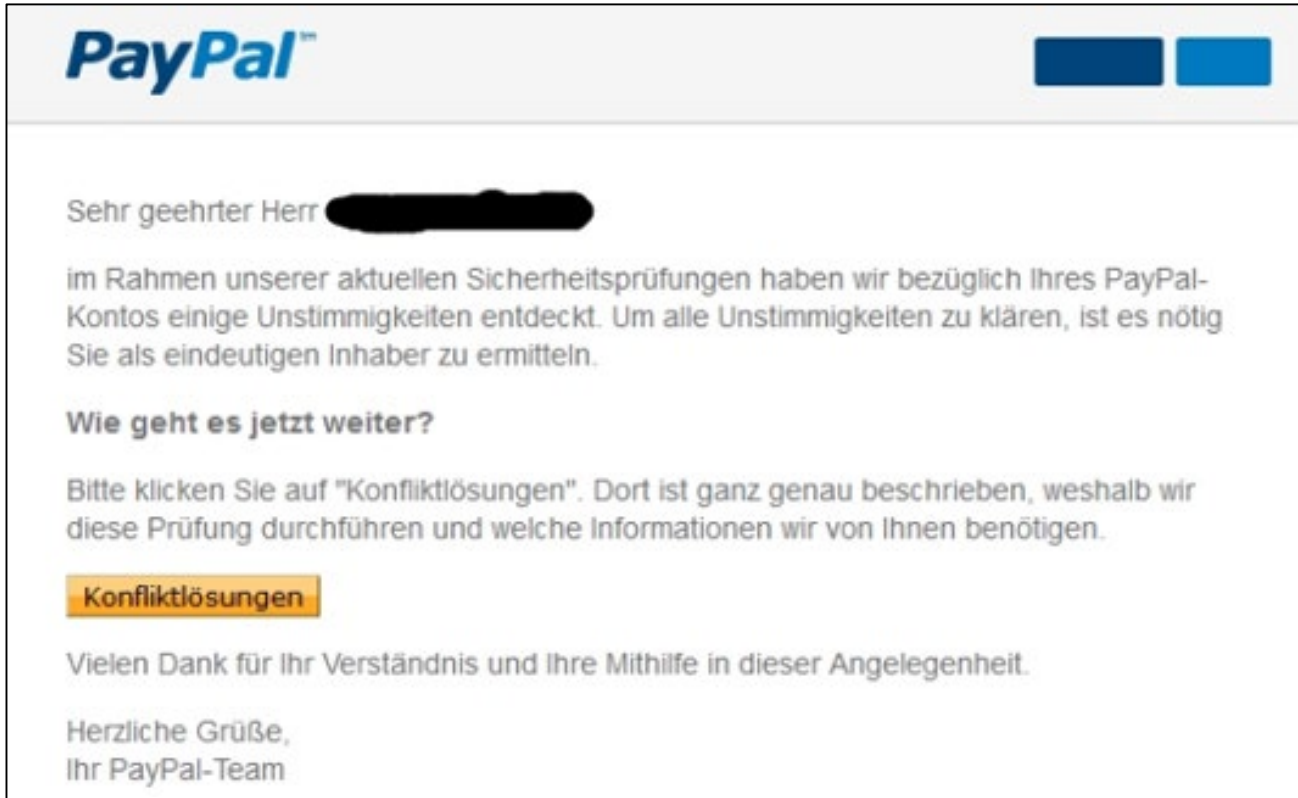
- Aufforderung die Nachricht an viele Menschen weiterzuleiten
- Betreff: Virus oder Warnung
- Bekannte Firmen (Facebook, Twitter,…) werden genannt

4. Erläutere, was eine Phishing-Angriff ist.

Phishing ist der Versuch über gefälschte E-Mails oder Webseiten Daten eines Benutzers (Passwörter, Kreditkartennummern, Zugänge zu Onlinebanking) für kriminelle Zwecke zu bekommen.

5. Woran kannst du einen Phishing-Versuch erkennen?

- unbekannte oder falschgeschriebene Absender
- häufig ist die Nachricht in einem schlechten Deutsch geschrieben
- unbekannte URL
- häufig unpersönliche Ansprache
- Rechtschreibung



6. Was ist eine digitale Signatur?

- Eine digitale Signatur ist eine elektronische Unterschrift. Hiermit wird der Benutzer identifiziert

7. Streiche den falschen Begriff durch, so dass eine richtige Aussage entsteht.

- Mit einem **privaten/ ~~öffentlichen~~** Schlüssel wird die digitale Signatur erzeugt.
- Mit dem **~~privaten~~/ öffentlichen** Schlüssel wird die Authentizität der Unterschrift überprüft.
- **Authentizität/ ~~Integrität~~** bedeutet, dass eine Nachricht eindeutig dem Absender zugeordnet werden kann.
- **~~Authentizität~~/ Integrität** bedeutet, dass der Inhalt einer Nachricht unverfälscht ist.
- **Verbindlichkeit/ ~~Integrität~~:** Der Absender ist tatsächlich der Verfasser der Nachricht und kann dies auch nicht abstreiten.

8b. Wie kann Tom nun richtig auf diese Phishing-Mail reagieren?

MAIL NICHT ERNST NEHMEN

- Keine enthaltenen Links anklicken
- Keine Anlagen öffnen
- PW ändern

9. Schaue im Internet nach, woher der Name SPAM kommt.

- *SPiced hAM*

(Marke die Dosenfleisch verkauft)

- SPAM= unerwünschte, in der Regel auf elektronischem Weg übertragene Nachrichten

10. Aus welchen Begriffen setzt sich das Wort Phishing zusammen? Du kannst danach googlen.

- Das Wort Phishing setzt sich aus den englischen Wörtern «Password» und «Fishing» zusammen.