Merkblatt Phishing-Angriffe erkennen

1. E-Mail-Missbrauch

Technische Schutzmassnahmen sind heute oft auf einem sehr hohen Niveau. Angreifer versuchen deshalb ihre Ziele über den Menschen als Schwachstelle zu erreichen. Sie bedienen sich des sog. Social Engineerings, also der zwischenmenschlichen Beeinflussung mit dem Ziel, beim Gegenüber bestimmte Verhaltensweisen hervorzurufen – die Preisgabe von vertraulichen Informationen, die Ausführung von Instruktionen auf Computern oder die Freigabe von Finanzmitteln. E-Mails sind ein hervorragendes Instrument zum Praktizieren von Social Engineering, da sich E-Mail-Absenderinformationen leicht fälschen lassen.

E-Mail-Missbrauch zeigt unterschiedlichste Ausprägungen. Immer wieder für Schlagzeilen sorgen Angriffe, bei denen E-Mails mit infizierten Anhängen (z.B. Office-Dokumente mit Makros) verschickt werden, die beim Empfänger sämtliche Daten verschlüsseln und damit dem Zugriff durch die Benutzer entziehen. Die Schäden, die dadurch entstehen können, sind immens – zum Teil ruinös. Nicht weniger gefährlich sind Phishing-Angriffe, die E-Mail-Empfänger zur Preisgabe von Login-Informationen verleiten sollen. Man spricht in diesem Zusammenhang von Identitätsdiebstahl. Phishing ist ebenfalls sehr weit verbreitet, da die Erfolgsaussichten hoch und die erbeuteten Identitäten wertvoll sind.

Mit einigen grundlegenden Verhaltensregeln lassen sich die Risiken von E-Mail-Missbrauch massiv reduzieren:

- Klären Sie die Echtheit von verdächtigen E-Mails beim Absender oder bei der Absenderin ab oder löschen Sie solche E-Mails sofort.
- Öffnen Sie nie Links oder Anhänge von verdächtigen E-Mails. Seien Sie besonders vorsichtig bei angehängten Office-Dokumenten (Word etc.), die Makros enthalten.
- Schützen Sie sich vor gezielten Phishing-Angriffen (dem sog. Spear Phishing): Gefälschte E-Mails, die gezielt für eine bestimmte Person erstellt werden (z.B. mit Informationen, die im Internet recherchiert worden sind), können sehr gut gemacht sein. Achten Sie deshalb auch auf Unstimmigkeiten in den Details.
- Lassen Sie sich nicht unter Druck setzen. Angreifer fordern immer wieder rasches Handeln, um ihre Opfer zur Vernachlässigung von Sorgfaltspflichten zu bewegen.

Auf den folgenden Seiten erhalten Sie Hinweise, wie Sie Phishing-Angriffe, d.h. Phishing-E-Mails und Phishing-Webseiten, erkennen können. Schauen Sie sich die Hinweise an und testen Sie danach Ihr Wissen anhand des Phishing-Tests von «eBanking – aber sicher!»

2. Phishing-E-Mails erkennen

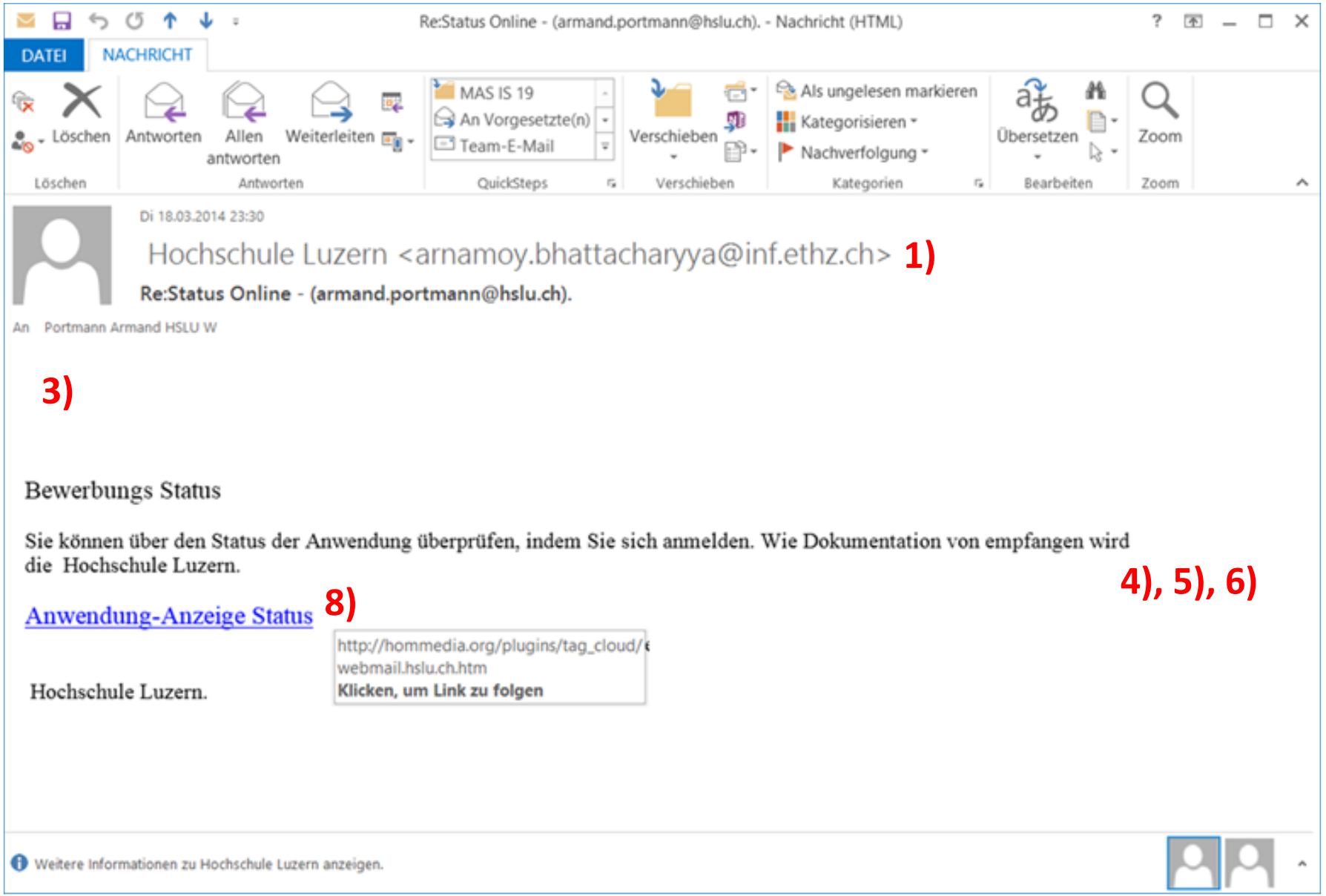
Phishing-E-Mails weisen sehr oft eines oder mehrere der folgenden Merkmale auf. Die aufgeführten Nummern referenzieren auf die Beispiel-E-Mails weiter unten im Dokument.

1. Anzeigename des Absenders und/oder Mailadresse des Absenders sind nicht korrekt[1].
2. Empfänger-Feld ist leer oder es werden fremde Namen anstelle des eigenen Namens angezeigt.
3. Anrede im Mailtext fehlt oder ist unpersönlich (z.B. „Sehr geehrter Kunde“).
4. Der Mailtext hat inhaltlich keine Bezüge zur angeschriebenen Person.[2]
5. Der Mailtext ist unverständlich, in schlechtem Deutsch oder eventuell gar nicht auf Deutsch formuliert.[3]
6. Der Mailtext enthält viele Rechtschreibfehler.
7. Der Mailtext enthält Schriftzeichen, welche in unserem Sprachraum nicht verwendet werden (z.B. Zeichen „ʒ“ anstelle von Umlauten).
8. Der eingebettete Link zeigt auf die Webseite des Angreifers, d.h. es ist eine falsche Webadresse hinterlegt. Diese falsche Webadresse kann sichtbar gemacht werden, indem die Maus ohne zu klicken über den Link geführt wird.[4]

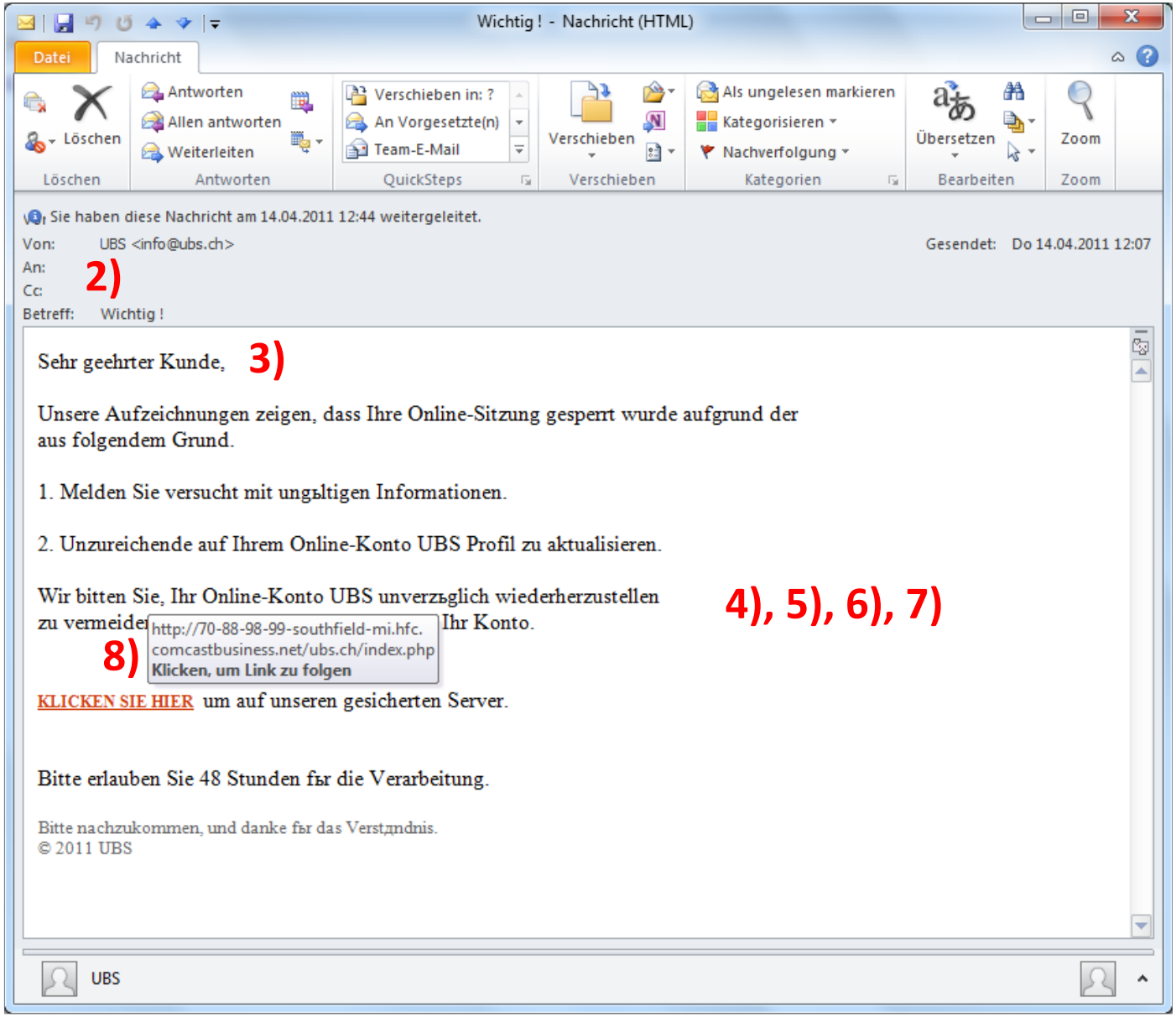
Wichtig: Mit Ausnahme von Merkmal 8 (falsche Webadresse im Link) muss keines der Merkmale in einer Phishing-E-Mail zwingend vorkommen, d.h. es gibt auch sehr gut gemachte Phishing-E-Mails!

[1] Interpretation von Mail-Absenderinformationen: Hans Muster <hans.muster@mustermail.ch> ➔ «Hans Muster» ist der Anzeigename; in spitzen Klammern steht die Mailadresse.
[2] Man wird z.B. als Kunde eines Finanzdienstleisters angeschrieben, pflegt zu diesem Dienstleister aber gar keine Kundenbeziehung.
[3] Dies ist vor allem dann sehr auffällig, wenn der angegebene Absender sonst in guter deutscher Sprache kommuniziert.
[4] Vgl. Anhang für die Interpretation von Webadressen.

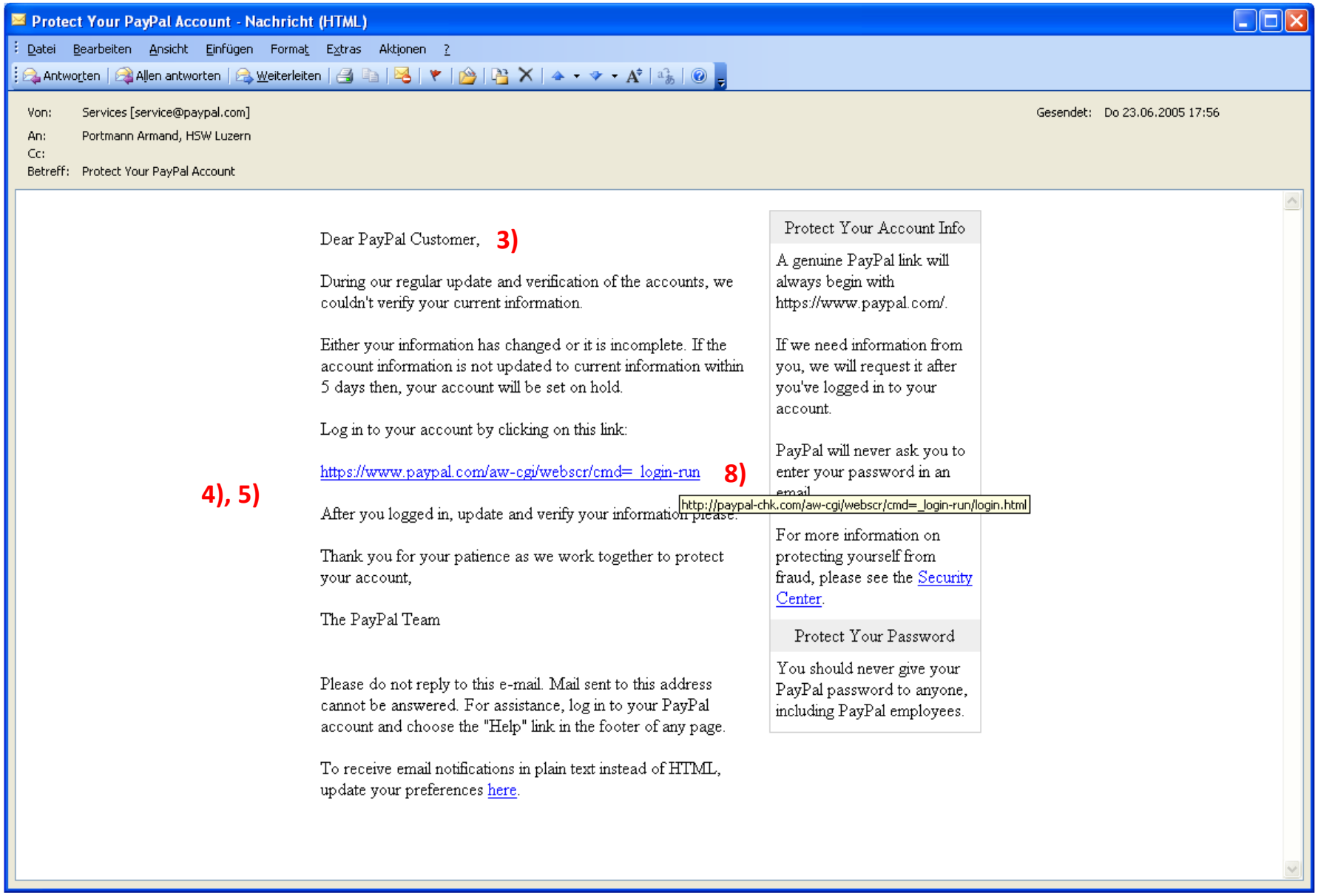
2.1. Beispiel-Mail 1: Phishing-Mail



2.2. Beispiel-Mail 2: Phishing-Mail



2.3. Beispiel-Mail 3: Phishing-Mail



3. Phishing-Webseiten erkennen

Bis vor kurzem konnten Phishing-Webseiten ziemlich einfach über fehlende Sicherheitsmerkmale im Browser erkannt werden: Der Protokoll-Indikator «http» wurde anstelle von «https» angezeigt und es gab kein Schlösschen in der Adresszeile. Heute verwenden die meisten Angreifer für ihre Phishing-Webseiten jedoch sichere Verbindungen, die im Browser mit «https» und Schlösschen gekennzeichnet sind. Die sichere Identifikation einer Webseite erfolgt deshalb neben der Überprüfung von «https» und Schlösschen zwingend über die Verifikation der Webadresse, die im Browser angezeigt wird.

Mithilfe der folgenden Überprüfungen kann eine Webseite als echt identifiziert werden – es liegt dann also keine Fälschung vor:

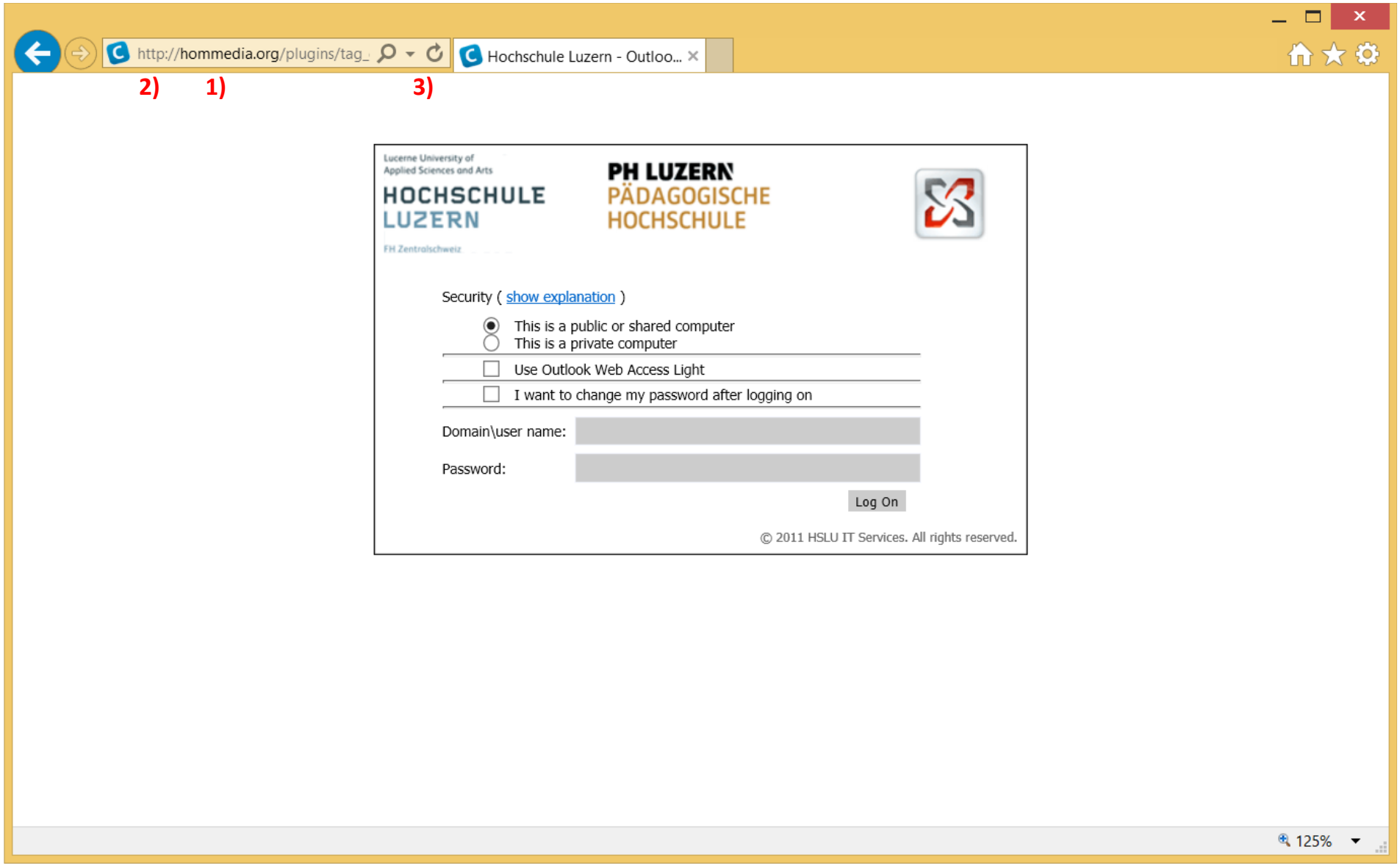
1. Angezeigte Webadresse ist korrekt.[5] (Dabei müssen nur die vom Browser fett hervorgehobenen Teile verifiziert werden.)
2. Protokoll-Indikator «https» wird angezeigt.
3. Schlösschen wird angezeigt.

Die Nummern der Aufzählung referenzieren auf die Beispiel-Webseiten, die folgen.

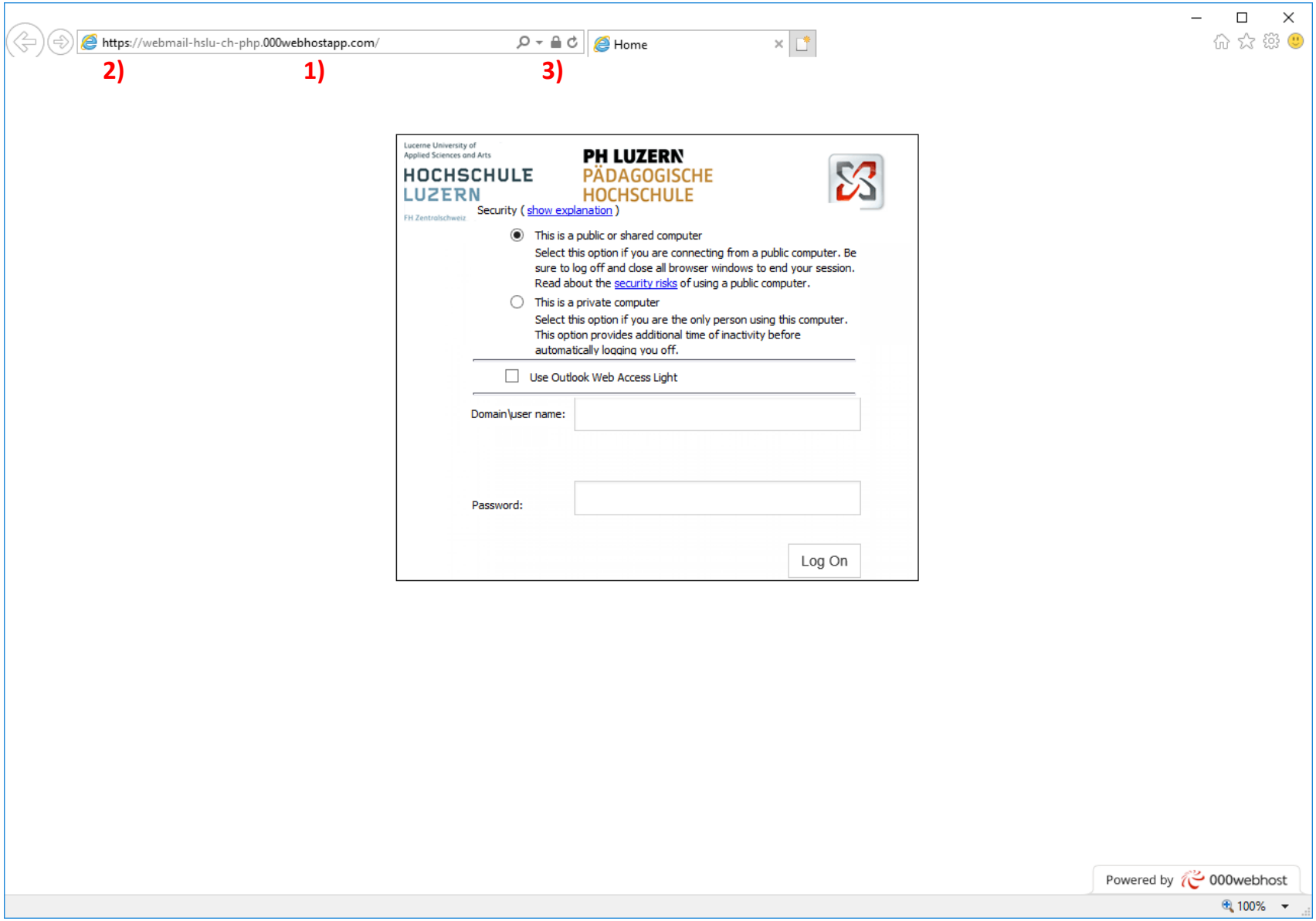
Hinweis: Nicht alle Browser zeigen die Sicherheitsindikatoren gleich an, z.T. werden Protokoll-Indikator und/oder Schlösschen *grundsätzlich nicht* angezeigt.

[5] Vgl. Anhang für die Interpretation von Webadressen.

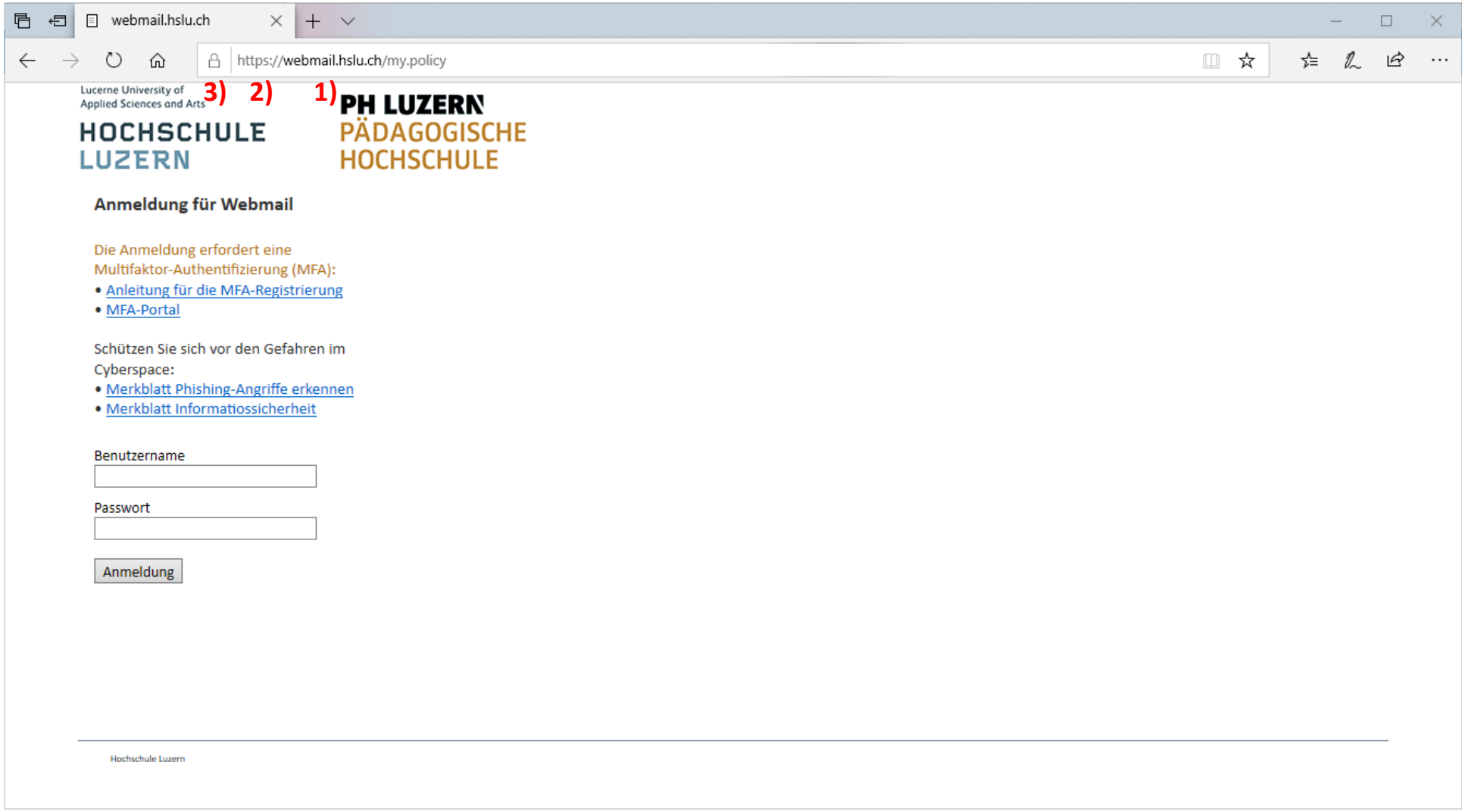
3.1. Beispiel-Webseite 1: Phishing-Webseite (Webadresse ist falsch, «https» und Schloss fehlen)



3.2. Beispiel-Webseite 2: Phishing-Webseite (Webadresse ist falsch, «https» und Schloss sind vorhanden)



3.3. Beispiel-Webseite 3: Echte Webseite (Webadresse ist richtig, «https» und Schloss sind vorhanden)



4. Anhang: Webadressen richtig lesen

Webadressen sind wie folgt aufgebaut:

http(s)://<HostID>.**<SecondLevelDomain>.<TopLevelDomain>**/<Path>

<SecondLevelDomain>	Teil der Adresse, der vom Betreiber der Seite gewählt wird und damit einen Bezug zum Betreiber herstellt.
<TopLevelDomain>	Teil der Adresse, der vom Betreiber der Seite gewählt wird und einen Bezug zu einem Land oder zum Inhalt der Seite herstellt.
<HostID>	Teil der Adresse, der für die lokale System-Identifikation verwendet wird. (Hier nicht relevant.)
<Path>	Teil der Adresse, der für die Navigation auf der Seite verwendet wird. (Hier nicht relevant.)

Beispiele:

https://www.**paypal.com/**home

<SecondLevelDomain>	**paypal**
<TopLevelDomain>	**com**
<HostID>	www
<Path>	home

https://www.**hslu.ch**/de-ch/

<SecondLevelDomain>	**hslu**
<TopLevelDomain>	**ch**
<HostID>	www
<Path>	de-ch