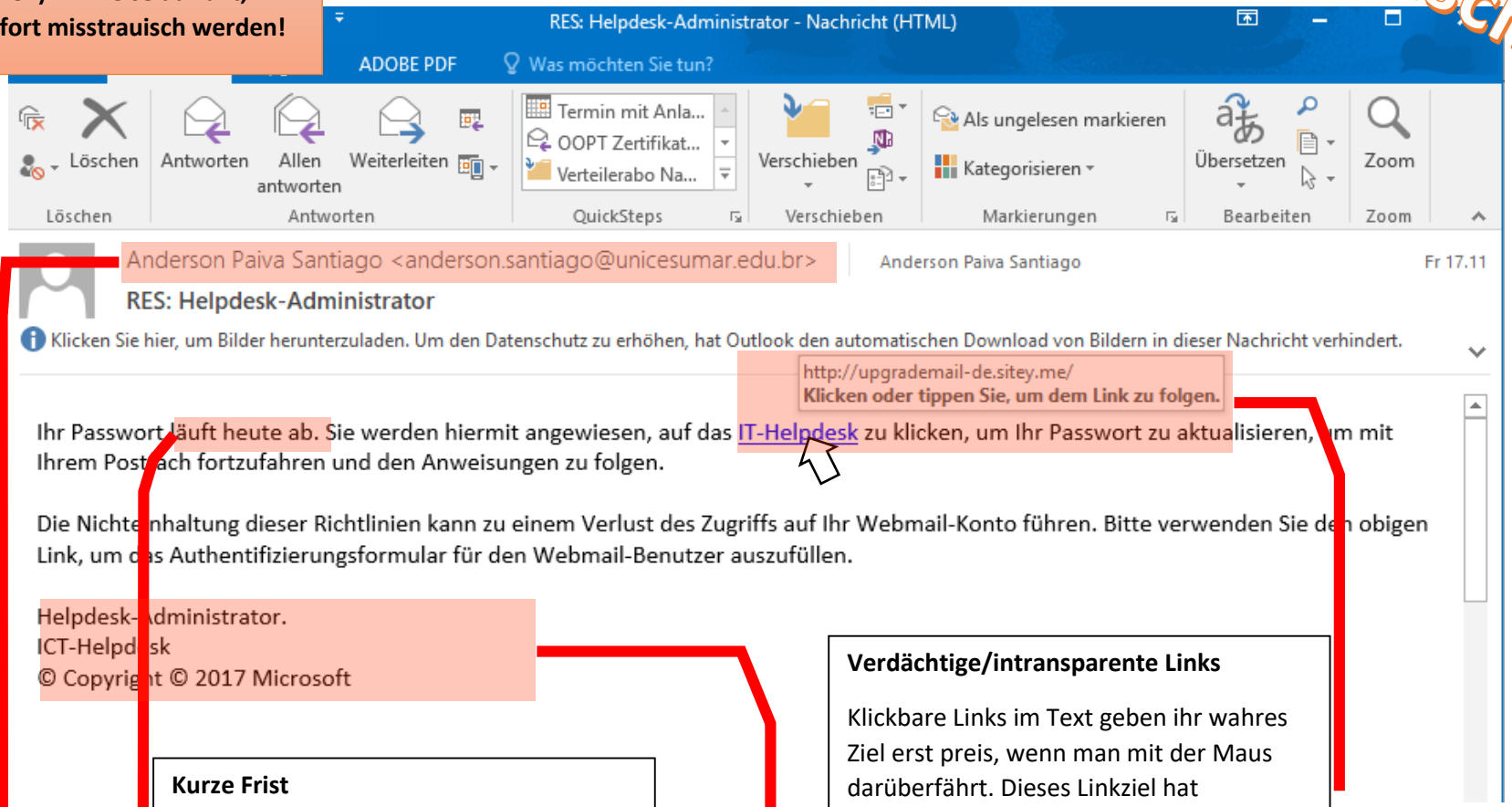
Wenn Ihnen auch nur ein einziger dieser (exemplarischen) Hinweise auffällt, sollten Sie sofort misstrauisch werden!

Gefälschte Mail



Kurze Frist

Seriöse Anbieter geben längere Fristen an; diese hier soll zu ***Kurzschlussreaktionen*** verleiten.

Verdächtige/intransparente Links

Klickbare Links im Text geben ihr wahres Ziel erst preis, wenn man mit der Maus darüberfährt. Dieses Linkziel hat offensichtlich nichts mit der Universität Siegen zu tun.

Unbekannter oder unerwarteter Absender

Hier ist es einfach, der Absender hat offensichtlich nichts mit der Universität Siegen zu tun.

Aber: Absender lassen sich problemlos fälschen! Selbst scheinbar bekannte Absender sind keine Garantie!

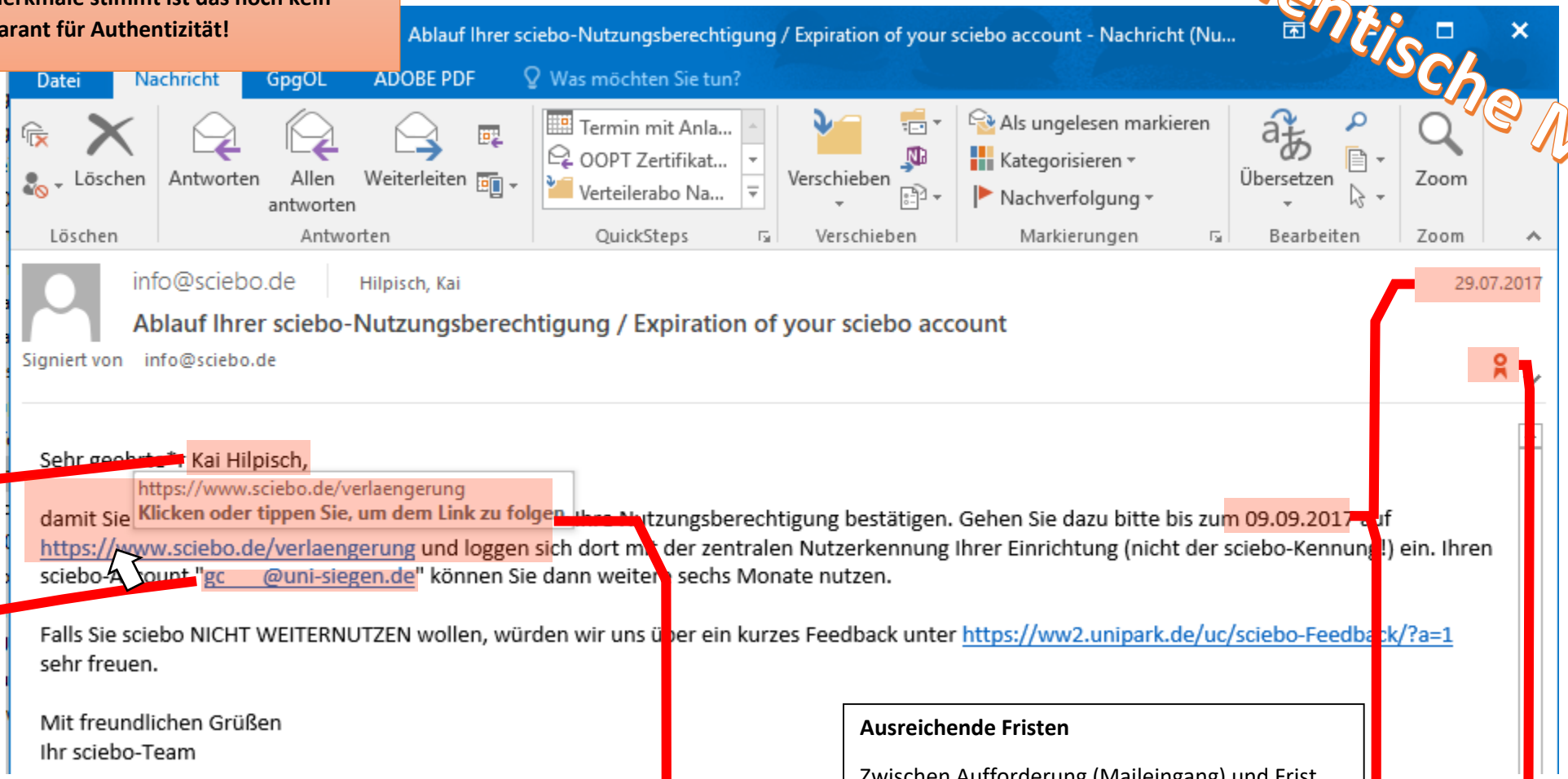
Generische Unterschrift / fehlende Kontaktinformationen

Diese Signatur gibt keinerlei bekannte Ansprechpartner oder sonstige Informationen. Der Verweis auf den Hersteller Microsoft soll Seriosität suggerieren.

Seriöse Anfragen beinhalten meist Optionen für z.B. telefonische Rückfragen, aber Achtung: Am Telefon kann auch ein Täter sitzen!

Insbesondere wenn nur eines dieser Merkmale stimmt ist das noch kein Garant für Authentizität!

Authentische Mail



Persönliche Ansprache, konkrete Bezugnahme

Der Absender der Mail verfügt offenbar bereits über bestimmte Informationen zu Ihrer Person und Ihrem Account, das deutet auf Authentizität hin.

Transparente, klar nachvollziehbare Links

Der Link und auch das angezeigte Link-Ziel gehören eindeutig zum genannten Dienst, das deutet auf Authentizität hin.

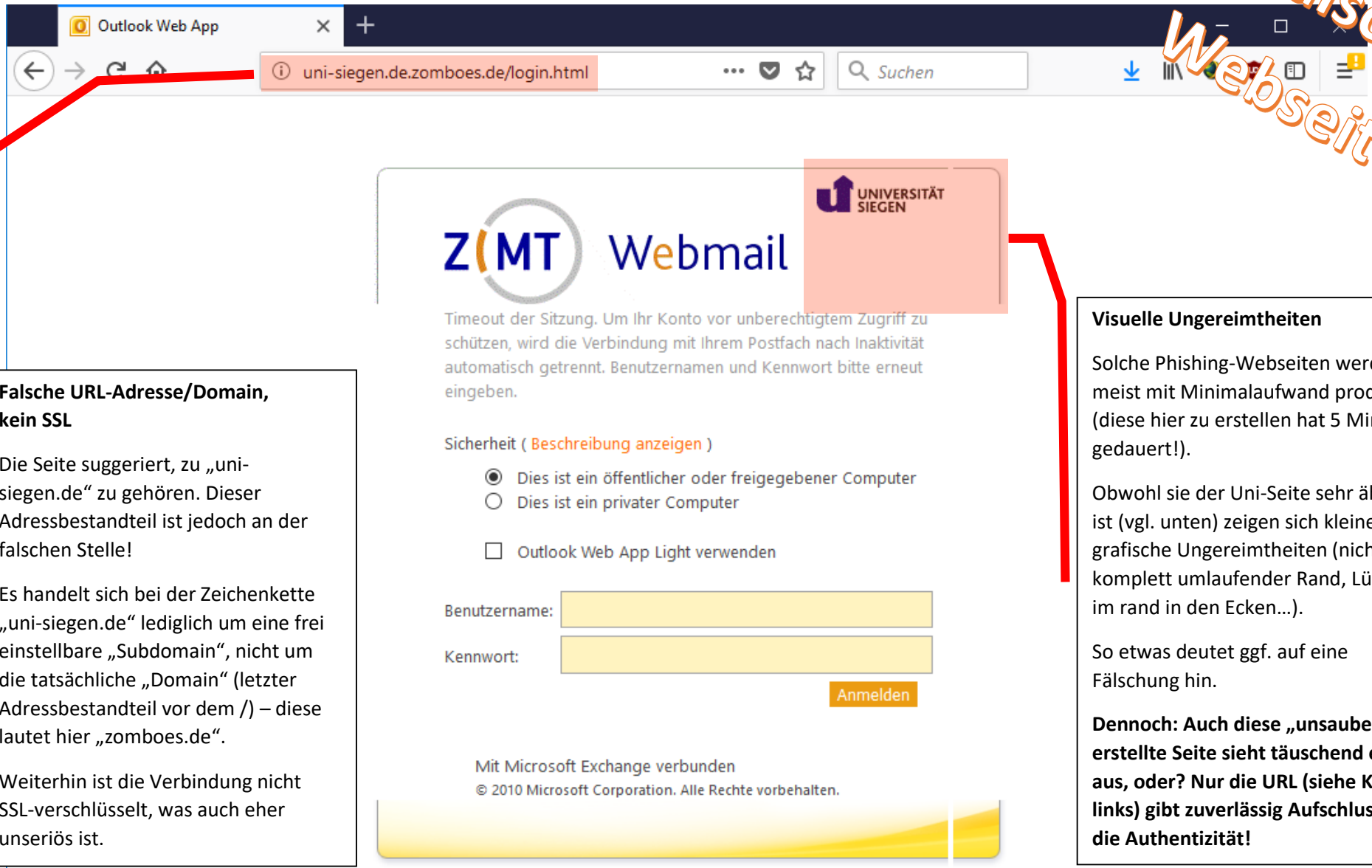
Ausreichende Fristen

Zwischen Aufforderung (Maileingang) und Frist liegt ein ausreichend langer Zeitraum.

Elektronische Signatur

Die Mail ist elektronisch signiert, das deutet auf Authentizität hin.

Gefälschte Webseite



Falsche URL-Adresse/Domain, kein SSL

Die Seite suggeriert, zu „uni-siegen.de“ zu gehören. Dieser Adressbestandteil ist jedoch an der falschen Stelle!

Es handelt sich bei der Zeichenkette „uni-siegen.de“ lediglich um eine frei einstellbare „Subdomain“, nicht um die tatsächliche „Domain“ (letzter Adressbestandteil vor dem /) – diese lautet hier „zomboes.de“.

Weiterhin ist die Verbindung nicht SSL-verschlüsselt, was auch eher unseriös ist.

Visuelle Ungereimtheiten

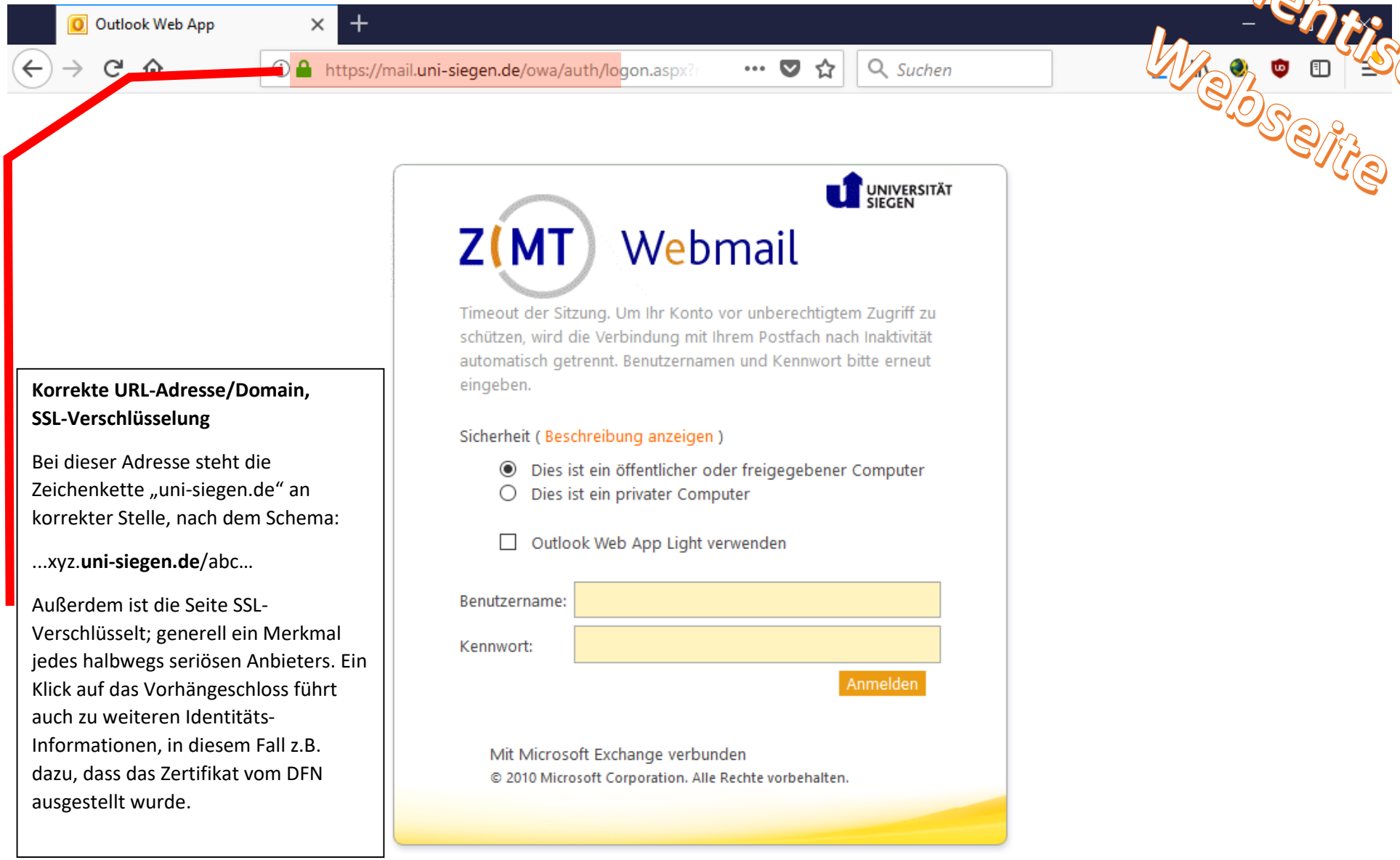
Solche Phishing-Webseiten werden meist mit Minimalaufwand produziert (diese hier zu erstellen hat 5 Minuten gedauert!).

Obwohl sie der Uni-Seite sehr ähnlich ist (vgl. unten) zeigen sich kleine grafische Ungereimtheiten (nicht komplett umlaufender Rand, Lücken im rand in den Ecken…).

So etwas deutet ggf. auf eine Fälschung hin.

Dennoch: Auch diese „unsauber“ erstellte Seite sieht täuschend echt aus, oder? Nur die URL (siehe Kasten links) gibt zuverlässig Aufschluss über die Authentizität!

Authentische Webseite



Korrekte URL-Adresse/Domain, SSL-Verschlüsselung

Bei dieser Adresse steht die Zeichenkette „uni-siegen.de“ an korrekter Stelle, nach dem Schema:

...xyz.**uni-siegen.de**/abc...

Außerdem ist die Seite SSL-Verschlüsselt; generell ein Merkmal jedes halbwegs seriösen Anbieters. Ein Klick auf das Vorhängeschloss führt auch zu weiteren Identitäts-Informationen, in diesem Fall z.B. dazu, dass das Zertifikat vom DFN ausgestellt wurde.