Verwaltungsdirektion
Informatikdienste
Marc Feer

Benutzerdokumentation für Studierende

Outlook Webmail 2013 (SPAM und Virenschutz)

Frohburgstrasse 3 · Postfach 4466 · 6002 Luzern
T +41 (0)41 229 50 10 · F +41 (0)41 229 50 20
helpdesk@unilu.ch
www.unilu.ch/IT

Outlook Webmail 2013

Verteiler	Alle Studierende	Version	1.01
		Revision	
		Erstellungsdatum	06. Oktober 2014
		Änderungsdatum	20. Oktober 2014
Verwendung	UNI intern		

Erstellt durch	Marc Feer, Jonas Zosso
Telefon	+41 (0)41 229 50 10
E-Mail	helpdesk@unilu.ch

Änderungsverzeichnis

Version	Datum	Autor	Bemerkung
1.01	20.10.14	M. Feer	Kap. 2.1

Referenzierte Objekte

Version	Datum	Autor	Bemerkung
1.01	24.9.14	M.Feer	Outlook Webmail 2013 Benutzerdokumentation für Studierende
1.01	24.9.2014	M.Rüttimann / M. Zehnder	Outlook Webmail 2013 (Konfiguration mit Apple Mail / Iphone)

22. Oktober 2014
Outlook Webmail 2013 (Umgang mit SPAM und Virenmails)

Inhaltsverzeichnis

1 Anmerkung 4

2 Massnahmen gegen SPAM und Virenbefall 4
2.1 Sicherheitsscans für E-Mails 4

3 SPAM 4
3.1 Funktion des „Junk-E-Mail Ordners“ 4
3.2 Offensichtliche Spam Emails 5
3.3 Mögliche Spam Emails 5
3.4 Mails als „Nicht SPAM“ klassieren 6

4 Phishing Mails 7
4.1 Wie funktioniert Phishing? 7
4.2 Wodurch erkennen Sie Phishing Mails? 7

1 Anmerkung

Bitte lesen Sie die Benutzerdokumentation „Outlook Webmail 2013“ um alle Funktionen kennen und nutzen zu können. Diese Dokumentation behandelt nur die Spamverwaltung.
Die vollständige Dokumentation finden Sie unter: http://www.unilu.ch/it.

2 Massnahmen gegen SPAM und Virenbefall

2.1 Sicherheitsscans für E-Mails

E-Mails sind leider häufig auch Transportvehikel für unerwünschten Inhalt wie Schadsoftware (z.B. Viren) oder unerwünschte Werbung (Spam).
Alle an die E-Mail-Domain "stud.unilu.ch" gesendeten, unverschlüsselten Emails und alle Emails, die über den Mailserver der Universität Luzern versendet werden, werden mit einer Anti Viren / SPAM Firewall über spezielle Software automatisch auf Computerviren und Spam geprüft und entsprechend klassiert.

Erkannte Viren oder andere Schadsoftware werden prinzipiell gelöscht. Bestimmte Dateianhänge, die als besonders gefährlich eingestuft werden müssen, werden ebenfalls gelöscht.

Achtung: Kein Spam- und Virenfilter arbeitet perfekt. Daher kann es vereinzelt vorkommen, dass erwünschte Mails als "Spam" oder "virenbefallen" beurteilt werden und umgekehrt. Die Informatikdienste der Universität Luzern können daher keine Gewähr übernehmen.

Um eine erfolgreiche SPAM-Bekämpfung zu gewährleisten verlässt sich die Universität Luzern auf Produkte eines führenden Herstellers. Diese befinden sich im Rechenzentrum der Uni. Es werden **keine Cloud Produkte eingesetzt.**
Die Spamerkennung wird durch verschiedene Techniken sicher gestellt, unter anderem sind dies DNS Realtime Blacklists, IP Reputation Lists, Sender- und Empfänger-Filterungen als auch Wörterkennungen.
Die Universität Luzern löscht keine Emails, entweder werden diese nicht angenommen oder zugestellt bzw. markiert („Tagged“) und in den Junk-E-Mail Ordner verschoben.

3 SPAM

3.1 Funktion des „Junk-E-Mail Ordners“

Es gibt bei jeder Spamfilterung einen „Graubereich“ wo die Schutzmechanismen eine Mail nicht genau klassieren können.
Damit diese Mails nicht aus Versehen gelöscht werden, werden solche Nachrichten mit **[Possible SPAM]** im Betreff markiert. Alle Nachrichten mit dieser Markierung werden direkt in Ihren **Junk-E-Mail Ordner** geliefert.

Mails in Ihrem Junk-E-Mail Ordner müssen Sie selber klassieren und den Absender entsprechend in Ihre White bzw. Black List eintragen. -> Siehe dazu Kap. 3.3

Sie müssen daher regelmäßig die Nachrichten im Ordner Junk-E-Mail überprüfen, um sicherzustellen, dass keine erwünschten Nachrichten verloren gehen.

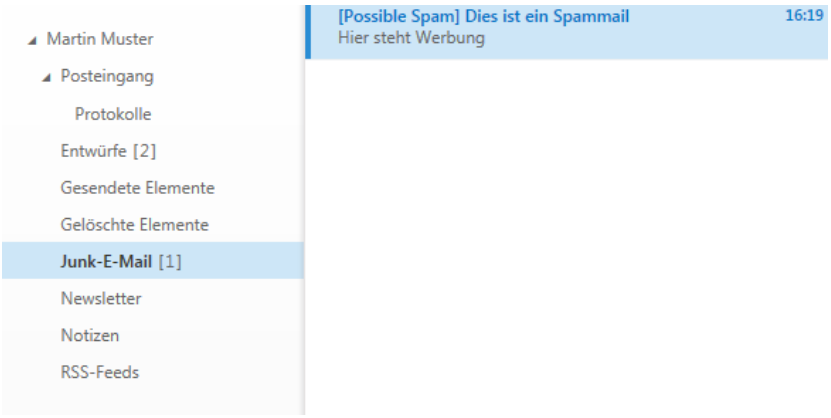
3.2 Offensichtliche Spam Emails

Offensichtliche Spam Emails werden nicht angenommen und zurück geschickt. Falls sich dennoch eine „saubere“ Email unter dieser Kategorie befindet, bekommt der Absender eine NDR-Meldung (Non delivery Report).
Leider zeigen nicht alle Freemail Provider diese NDR an (u.a. Google Mail)

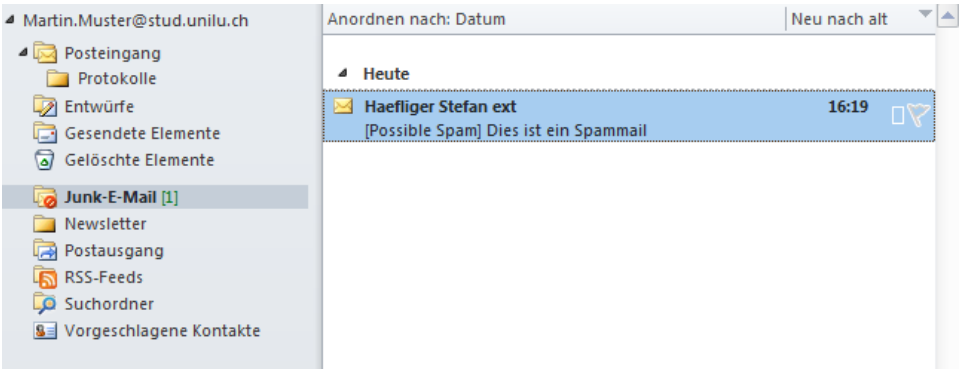
3.3 Mögliche Spam Emails

Unter diese Kategorie fallen Emails, welche nicht sicher als Spam oder „richtige“ Emails eingestuft werden können.
Solche Emails werden automatisch mit der Bezeichnung **[Possible SPAM]** im Betreff versehen und in Ihren Junk-E-Mail Ordner verschoben.

Hier ein Bespiel in „Outlook Web Access“

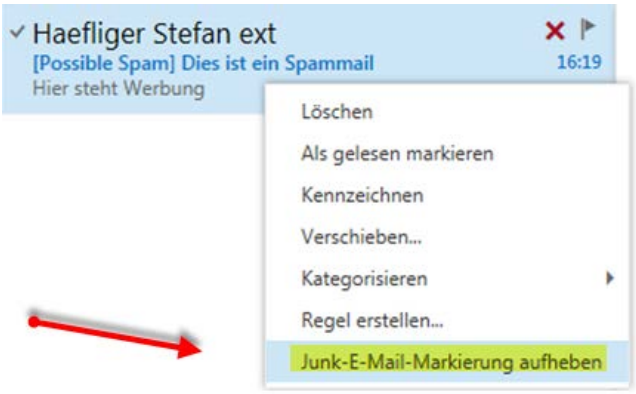


Hier ein Beispiel in „Outlook 2010“



3.4 Mails als „Nicht SPAM“ klassieren

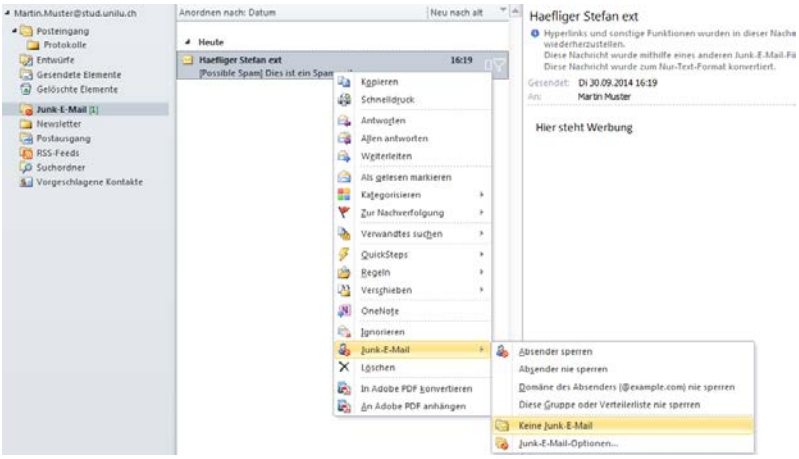
Sollte es sich nun um eine „Falschklassierung“ handeln, und Sie sich sicher sind, dass die Mail keine SPAM-Nachricht ist, können sie mittels Rechtsklick diese Nachricht in den Posteingang verschieben. „Junk-E-Mail-Markierung aufheben“



Wenn sie die Junk-E-Mail Markierung aufheben, wird der Absender dieser Mail automatisch in die Liste der zugelassenen Absender eingetragen (White-List).

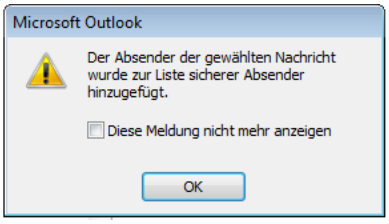
Falls Sie Outlook 2010 oder 2013 auf Ihrem Laptop installiert haben und sie Studmail mit beispielsweise „Outlook Anywhere“ (Siehe Doku „Outlook Web App 2013 Kap. 5.2) konfigurierten, haben Sie weitere Möglichkeiten Ihre Mails zu klassieren.

Beispiel Outlook 2010:



- Absender sperren
- Absender nie sperren
- Domäne des Absenders nie sperren (Beispielsweise: @unilu.ch)
- Gruppen oder Mails von Verteillisten nicht sperren

Wenn sie “Absender nie sperren“ wählen, wird dieser Absender als sicher angesehen und seine E-Mails werden nicht mehr als Spam eingestuft.



4 Phishing Mails

Der Begriff Phishing leitet sich von dem englischen Wort "fishing" (angeln) ab und beschreibt das Fischen nach persönlichen Daten. Die Ersetzung des Buchstabens "F" durch "Ph" lässt sich aus der Kombination der englischen Worte "password" (Passwort) und "harvesting" (ernten) erklären.

4.1 Wie funktioniert Phishing?

Phishing-Attacken beginnen immer mit dem meist massenweisen Versand von Phishing-Mails an beliebige Empfänger. In diesen **seriös wirkenden Schreiben** mit **gefälschten Absender-Adressen** werden die Empfänger unter **einem Vorwand** aufgefordert Benutzernamen, Passwörter oder E-Banking PIN/TAN mitzuteilen. Entweder durch Ausfüllen eines **Formulars** direkt in der E-Mail oder zum **Anklicken eines Links** der zu einer gefälschten Webseite führt, die **genau wie eine Originalseite des vermeintlichen Mail-Absenders aussieht.**

4.2 Wodurch erkennen Sie Phishing Mails?

- **Weder die Informatikdienste der Universität Luzern, noch Ihre Bank, Post, oder Auktionshäuser wie Ebay, Ricardo etc. werden Sie auffordern Benutzername und Passwort in einem Mail oder via Link mitzuteilen!**
- **Die Absenderadresse ist falsch.**
- Der **Link** im Mail entspricht nicht der Absenderfirma.
- Unter einem meist **dringenden** Vorwand wird der Empfänger aufgefordert, **schnellstmöglich** eine Handlung auszuführen. Oft wird angedroht, bei Nichtbefolgung der Anweisung würde etwas Schlimmes oder Unangenehmes geschehen, z.B. der Zugang würde gesperrt bzw. gelöscht.
- Die **Anrede** in Phishing E-Mails ist **meist unpersönlich**, wie z.B. "Sehr geehrter Kunde" oder "Sehr geehrtes Mitglied".
- Die ersten Phishing E-Mails wiesen noch **grobe Rechtschreib- oder Grammatik-Fehler** auf. Inzwischen haben es die Phisher jedoch gelernt, nahezu fehlerfreie E-Mails zu verfassen. Mitunter werden jedoch noch immer ungebräuchliche Formulierungen verwendet oder **Umlaute sind nicht korrekt dargestellt.**