HOCHSCHULE LUZERN

IT Services Support

How to avoid spam

Short description:	Definition of "spam" What to do to avoid spam.

Classification: ☒ IT internal   ☒ Public
                   ☐ Other

Customer group: ☒ HSLU   ☒ PHLU
                   ☐ Other

Function: ☒ Employees/lecturers ☒ Students
                   ☐ Other

Device management type: ☐ HSLU/PHLU devices ☐ Private devices
                   ☐ Other

Operating system: ☐ Windows   ☐ Mac
                   ☐ Other

Publication: ☒ hslu.ch/helpdesk ☒ Intranet
                   ☐ Other

Support:
Web: hslu.ch/helpdesk
Email: informatikhotline@hslu.ch
Phone: 041 / 228 21 21
Portal: helpdesk.hslu.ch

List of changes

Version	Date	Status	Changes and remarks	Edited by
No 0.1	12/06/2013	Draft	Created	len
No 1.0	24/06/2013	Final	-	buc
No 1.1	04/09/2013	Adjustments	Adjusted to match default template	vog
No 2.0	28/06/2017	processed	Transferred to Docunize	nil

Table of contents

1. What is spam?

Spam messages are unwanted, unsolicited and generally electronic messages that often have promotional content.

2. Guidance on handling spam emails

2.1. Sharing of email addresses

2.1.1. Do not share your email address on the internet

Often, online forums require user registration with an email address. It is advisable to create an extra (and free) email address for this kind of thing, for instance with GMX, GMail, Yahoo or another service.

2.1.2. Do not make guestbook entries

Spammers trawl guestbooks for email addresses. Either don't enter an email address or, if required, use an extra address created for the purpose.

2.1.3. Do not share email addresses or phone numbers

Often, customer information is sold on, which might lead to a surge of spam emails and promotional phone calls For this reason, it is advisable to only ever share the information required, and nothing on top of it.

2.1.4. Do not send any email greeting cards

The information gathered is often sold on to third parties, which means both the sender and the recipient of the card end up receiving lots of spam.

2.1.5. Do not accept services by websites

Do not use any *Share with your friends* types of feature. Instead, copy the URL of the website in question and send it to the intended recipient by email.

2.2. Handling of other people's email addresses

2.2.1. Do not share other people's email addresses

Never share anybody's email address without consulting them first.

2.2.2. Use the BCC feature for mass emails

If you need to send out mass emails, make sure to copy the recipients' addresses into the "BCC" (blind carbon copy) field so that they cannot see each other's addresses.

Activating the BCC field in Microsoft Outlook: https://support.microsoft.com/kb/299804/de

2.3.   Handling of received spam emails

2.3.1.   Immediately delete and never open spam emails
By clicking on or opening spam emails, the reception of the email and, with it, the validity of your email address will be confirmed to the spammer. The email address will then be considered verified and sold on to third parties, which leads to even more spam.

2.3.2.   Never click on any links in spam emails
Many of these links lead to websites contaminated with malware (viruses, Trojans, etc.).

2.3.3.   Ignore "unsubscribe" features in emails
Ignore "unsubscribe" features in emails such as *If you no longer wish to receive our free newsletter, click [here]*. By clicking on this message, you will confirm to the spammer that your email address is, in fact, valid.

2.3.4.   Never reply to spam emails
Sender addresses in spam emails are generally fake, i.e. a reply will end up nowhere or with an unrelated person.
However, should the spammer have used a functioning address, a reply will only lead to the verification of the victim's email address and used for even more spam emails.

2.3.5.   Never open any spam email attachments
Spam email attachments are often contaminated with malware (viruses, Trojans, etc.).

2.4.   Use several email accounts
Only ever share personal or business email addresses with friends, family, colleagues, etc. Create an extra (free) address with e.g. GMX, GMail or Yahoo to sign up on websites or for similar activities.

2.5.   Use the spam filter of your email software
Most email software comes with its own integrated spam filter. It can be adjusted and trained by marking spam emails as such. Emails that have wrongfully ended up in the spam folder can be marked as *no spam*.
If your email programme of choice has no spam filter, you can install one yourself. Some email applications (e.g. Outlook) allow for the blocking of specific sender addresses.

Free-of-charge spam filter for Microsoft Outlook and other programmes:
http://www.spamfighter.com/SPAMfighter/Lang_DE/Product_Info.asp