phishing

I received a phishing mail: What to do?

- Delete it.

I received a mail and I'm unsure if it is a phishing mail

- (1) Check our IT news: https://math.uzh.ch/my - we're publishing phishing mails there, as soon as we're aware of it.
  - Announcements starting with '[Phishing] ...' means: **this is a phishing mail, delete it**.
- (2) If (1) does not show the current mail, wait 1 hour, check again - still not listed? Forward the mail to support@math.uzh.ch and ask if it is a phishing mail.

Indicators of a phishing mail

- (3) Does the mail ask you to click on a link and/or to login somewhere?
- (4) Do you requested support from the sender?
- Still wondering if it is a phishing mail? Check the links inside of the supiscous mail.

Links (URL) in the suspicous mail

- (5) Move the mouse over any given URL (don't click, just hover).
  - This does not work on a mobile phone. Use a computer.
  - In the lower left corner you'll see the **real** URL.
  - Only judge the URL shown in the lower left corner, not the one directly shown in the mail!
- Does the Text (or URL) in the mail and the real URL (lower left corner) match? Yes: that's a good sign.
- (6) For regular users, it's hard to distinguish between good and bad URLs.
  - Typical URL: https://wiki.math.uzh.ch/public/books/public-wiki/chapter/email

- Look ONLY on the first part, this means up to the first single '/' (very important!). In this case: https://wiki.math.uzh.ch - is this known to you?
- Example of bad URL: http://3.0.138.238/home... this is not trustworthy.

People recieve mails form me, but I didn't send them

- The email protocol is very insecure - especially regarding the sender address.
- Every person (even you), can configure any address as sender and/or reply-to address.
- This typically does **not** mean your account has been hacked.
- Instead someone configured your address as sender address. That's all.
- There is nothing you can do against it.
- As a reference: How much SPAM have you already received by *real* people?
  - Often, the shown name and email address is just a random grabbed one.
  - Better organized phishing campaign uses sender email adresses from the same organization which will be attacked - this increases the probability that the phishing will be treated as authentic. Meaning: Don't blindly trust `...@uzh.ch`-addresses.

What is a phishing mail?

An attacker tries to get your username/password by providing a website with a login box. Such a site will save your credentials. They often look identical to known websites.

What happens if I provided my credentials to a phishing site?

- Thousands of people will receive spam, because your credentials will be misused to send spam. You're **reponsible** for this!
- The UZH will be marked as 'spammer' - UZH mail will be marked as potential spam or the receiving of UZH mail is completely **denied**.
- After submitting your credentials, it takes only a few minutes until the SPAM sending process starts.
- If you realize something went wrong - change your I-MATH password immediately and contact us.

I can't open my mails anymore

- If we're seeing too much traffic on an account, we lock the account. This is the only way to securely stop sending further mail by the spammer.
- We won't contact you: because you won't be able to read our mail anymore. **You have to contact us** (by your private email or via chat https://hello.math.uzh.ch).

'Do not trust any email' means ...

- Do not trust any **email address** - this is not a joke. Don't do it.
- Do not trust any **content** - see below 'Personalized...'.

Personalized Spam Mails by Big Data & AI

- An attacker starts some 'big data' algorithm which reads a hacked email inbox, the collected email adresses (auto addressbook) and correlates that with other information like hacked email accounts, computer (incl. PDF, word or excel files saved on the computer) or general public available information.
- A personalized email is built automatically and fits perfectly to **your** current situation, but it's still a fake.
- With the advent of AI, personalized phishing mails become very easy to generate.

Personalized Spam Mails by a Human Bad Actor

- With the hacked collected information and some creativity: There are almost no limits to creating convincing phishing mails.
- Yes, this is a real problem. Targeted attacks can be very effective.
- Result: Be very suspicious. Ask for help in evaluating an email by forwarding it to us. (support@math.uzh.ch)

Should I stop using email?

- No - Email is by far the most accepted electronic way to communicate - keep it.
- Just be aware that an email behaves like a postcard: everyone can write it, with any sender address, with any information.

Are there alternatives to email?

Yes: use a service which guarantees the identity of a sender.

- Signed email: this is not commonly used but possible. We do not support those.
- I-MATH members: use https://hello.math.uzh.ch - this is our secure chat server.
- Decide on your own to use messengers like Signal, Threema, Telegram, Wire, !WhatsApp

---

Revision #5
Created 2026-06-30 10:54:22 CEST by admino
Updated 2026-07-03 15:28:16 CEST by Jonas Valentin Rose