Karlsruhe Institute of Technology

E-Mail Security

Spam, Phishing, and Malware

IT SECURITY

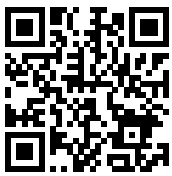
In a Nutshell

In this leaflet, we address three kinds of harmful e-mail:

- **Spam** is unsolicited e-mail containing junk advertisements or other useless content. Its primary harm is the time spent handling it.
- **Phishing** e-mail is an attempt to lure you into disclosing sensitive information, such as your KIT account access data.
- E-mail containing **malware** either as an attachment or as a link.

If You Are Receiving Spam

- You may simply **ignore** spam e-mail. The less time you spend on it, the better.
- You may also report spam e-mail to the SCC. By doing so, you help improve the central spam filters. Please refer to the **spam reporting program** for more information:



https://www.scc.kit.edu/sl/spam_en

If Spam is Being Sent in Your Name

You are receiving a lot of refusal notices that look like spam is being sent via your KIT account? Fortunately, this is usually not the case: To slip through spam filters, attackers fake the return address of the spam they send. For this, they use real, existing addresses. As with physical mail, this is impossible to prevent.

Usually, such a wave of refusal notices will only last for a few hours—you just need to have a little patience and wait it out.

How to Protect Yourself

- Keep your operating system and applications up to date. Make sure to apply all security patches as soon as they are available.

https://www.scc.kit.edu/sl/patch_en

- Disable the execution of macros in office documents.
- Make sure your virus protection is adequate. The KIT offers an antivirus solution:

https://www.scc.kit.edu/sl/antivir_en

How to Tell if an Attack Has Been Successful

- Did you disclose your password via e-mail or on a web site?
- Did you open an e-mail attachment that you now have second thoughts about?
- Did you click on a link that lead to different content than you expected, unexpectedly asked for your credentials, or asked you to download something?

These are possible indicators of an attack. If in doubt, contact your IT officer (ITB). In case of concrete suspicion, please also contact the KIT-CERT which assists you in dealing with IT security incidents.

Harmful E-Mails: A Danger to the KIT

As a scientific institution, the KIT is in a particular situation—on one hand, we act in public, but on the other hand, we have to protect some information from others. For you as a KIT member, communication—in particular via e-mail—is essential for your work. Therefore, e-mail is a gateway commonly used by attackers.

Attackers seek to gain access to your data and IT systems. To reach their goal, they try to coerce you into opening malicious e-mail attachments or web links.

There is no way to prevent these attacks completely by technical means without seriously impairing your ability to work. Thus, **sensible user behavior** is an important part of the IT security process of the KIT.

This leaflet offers you some important information about this.

If You Are Receiving Malicious E-Mails

- The easiest and fastest way to deal with malicious e-mail of any kind is to **ignore** and **delete** it.
- Inbound e-mails are scanned for spam content automatically and marked accordingly. E-mails tagged as spam are then moved into a separate e-mail folder if you have activated this service.
- Occasionally, spam is not properly recognized. You can help us improve the detection by moving such e-mails into the **spam reporting folder**. The spam filter will then be trained with these e-mails.

How to Recognize Phishing or E-Mails with Malware

Phishing e-mails try to feign a legitimate purpose in order to trick you into revealing sensitive data—for instance, your KIT password.

Attacks with malware aim to get you to run malicious software on your computer. This in turn allows the attacker to do further damage, for example by encrypting your hard drive.

It is very hard to recognize a careful attack. The following questions may help you to reach a decision as to whether a given e-mail is part of an attack:

- Was receiving the e-mail a surprise to you?
- Is the greeting incorrect or does it not fit the recipient address?
- Have you never before had any correspondence with the sender?
- Are you being asked to disclose private information?
- Does the sender try to pressure you? "If you don't reply immediately, we'll suspend your account!", "Your computer is at risk!", …
- Do links contained in the e-mail point to different websites than claimed? Note that your e-mail client is able to display the target of a link without opening it.
- Is the request either very generic or very detailed but references a process completely unknown to you?
- Does the e-mail contain attachments with generic names like "invoice-2752.zip" or "urgent.exe"?
- Does the topic not fit your work context?
- If a stranger approached you at your doorstep with the same question, would you feel uneasy about disclosing the requested information?
- Did the sender use a KIT e-mail address but did not digitally sign the e-mail?

The more questions you answer with "yes," the more likely it is the e-mail is part of an attack.

If in doubt, try to contact the alleged sender via other means.

By the way, these plausibility checks are also applicable to telephone calls, faxes, and regular mails.

How to Protect Yourself

You can improve your protection from malicious e-mail by applying the following general rules:

- If you think an e-mail is malicious, simply ignore and delete it.
- If you are uncertain, try to contact the alleged sender of the e-mail.
- The SCC will **never** ask you to disclose your password to anybody. Should this ever happen, it is a security incident—please inform the KIT-CERT immediately! Details on how to contact the KIT-CERT can be found on the back of this leaflet.
- Keep the operating system and the application software on your computer at the current patch level at all times. Doing so minimizes the attack surface of your system.

https://www.scc.kit.edu/sl/patch_en

- Make sure to have adequate virus protection in place and keep it up-to-date. The antivirus software package offered by the SCC can be found here:

https://www.scc.kit.edu/sl/antivir_en

- You can help us improve our e-mail filters by actively participating in the spam reporting program.

https://www.scc.kit.edu/sl/spam_en

- If you suspect a concrete attack, please contact the KIT-CERT.

What to Do if Things Went Wrong

Well-prepared and well-executed attacks are very hard to recognize. Therefore, it is always possible that sensitive data is disclosed or systems are compromised.

If you suspect this to be the case, please see your IT officer (ITB) and the KIT-CERT right away. The KIT-CERT will assist you in handling IT security incidents and can coordinate incident response. This is imperative to avoid further damage to your data and the IT infrastructure of the KIT.

KIT CERT

Contact

Karlsruhe Institute of Technology (KIT)
The IT Security Officer

Andreas Lorenz

Campus North: Building 441, room 222
Campus South: Building 20.21, room 306

Phone (CN): +49 721 608-24500
Phone (CS): +49 721 608-46637
E-mail: itsb@kit.edu

www.itsb.kit.edu

KIT Computer Emergency Response Team (KIT-CERT)

Phone: +49 721 608-45678
Fax: +49 721 608-9-45678
E-mail: cert@kit.edu
Jabber: security@conference.kit.edu
Web chat: https://security-chat.cert.kit.edu

www.cert.kit.edu

Publisher

Karlsruhe Institute of Technology (KIT)
Kaiserstraße 12
76131 Karlsruhe
Germany
www.kit.edu

2018-08-21 (revision 20/cd6ef5c)