E-mails have long been a key point of attack for those seeking to spread malware, but they also provide a useful platform for attempts to extort or defraud the recipient as well as for phishing. Thanks to regular media coverage, that's something of which we're all aware. Despite this, there are still repeated incidences of companies sustaining considerable damage as a result of data loss or the disclosure of sensitive information. Although antivirus software and diligently updating installed software helps to mitigate some of these risks, there is no such thing as 100% security. When using e-mail, awareness of these threats helps us and UZH as an institution to prevent potential loss.

Attackers are interested in the following information or targets:

- Personal information about you, including account login information, credit card details, your address, etc.
- Usable information on and about your PC or MAC, such as vulnerable software versions and sensitive personal data, etc.
- The forwarding of information to a service outside the UZH domain, so that all of the data that is transmitted can be intercepted and potentially manipulated or sold
- Ways in which to infect your PC or MAC with malware (e.g. via vulnerable software versions), in order achieve one of the aforementioned objectives or to gain remote access
- Gaining administrator rights in order to penetrate deeper into an organization's infrastructure

What Is Phishing?

Phishing is a simple yet dangerous attack. It's likely that we have all received a phishing mail at some point. They can be very poor and primitive, or look deceptively genuine. They contain a link to a website, or an attachment, and you will generally be asked to enter a password. Phishing attacks have become increasingly effective in the recent past, as the fake messages have become more and more authentic-looking, with fewer and fewer spelling mistakes. The same is true when you are redirected to a website which is indistinguishable from the original, right down to the URL.

The Five-Second Security Check

You can reduce risks considerably with a simple five-second security check. The five critical points that you should consider before you open any attachment, click on any link, or answer the e-mail are the following: sender, subject line, content, links and attachments:

- Do you know the sender?
- Does the sender's name match the e-mail address?

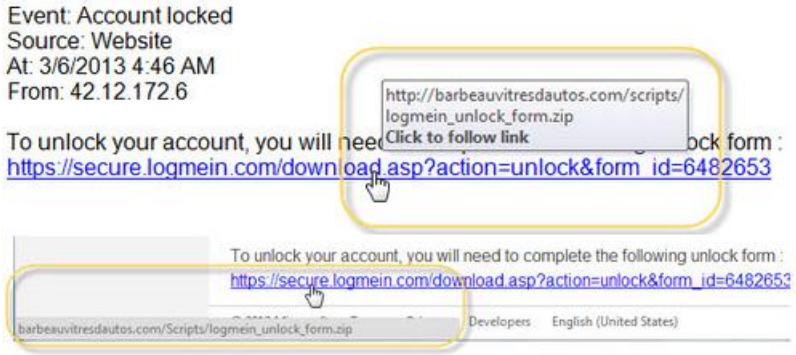
Example – fake address:
From: UNIVERSITY OF ZURICH uzh bianoda@adv.oabsp.org.br

The name of the sender bears no resemblance to the e-mail address, and in this case has nothing to do with the University of Zurich.

- Does the subject line make sense?

Be particularly vigilant if you notice any of the following content:

- An impersonal salutation
- Spelling and grammatical errors / awkward writing style
  If the sender is a manager or someone else you know, does the writing and sign-off match their usual style? (Please confirm the transfer...Cheers...)
- Language that is not typical in Switzerland
- A URL that does not match the link that is given
  In this example, the link actually takes you to a page that differs from the supposed original (move your cursor over the link, but do not click!)



- Attachments – are you expecting an attachment from this sender?
- Payment orders – even if these appear to come from your line manager, if you are in any doubt check with them in person
- Questions concerning sensitive data, such as passwords
- A clear warning sign is if the e-mail tells you that the data must be entered within a short time-frame
  For example: "If you don't pay within the next three days, your account will be suspended", or the e-mail contains phrases such as "your account has been manipulated" or "urgent action required".

Together, these questions will give you a good idea as to whether or not you can regard the e-mail as trustworthy. Good common sense, above all, is what is needed here. If the five-second check indicates that all is not as it should be, please contact your IT support staff, the UZH Service Desk or It-sicherheit@zi.uzh.ch directly. If you are in any doubt, do not open any attachment, click on any link or reply to the e-mail.

How Do I Recognize Dangerous Attachments?

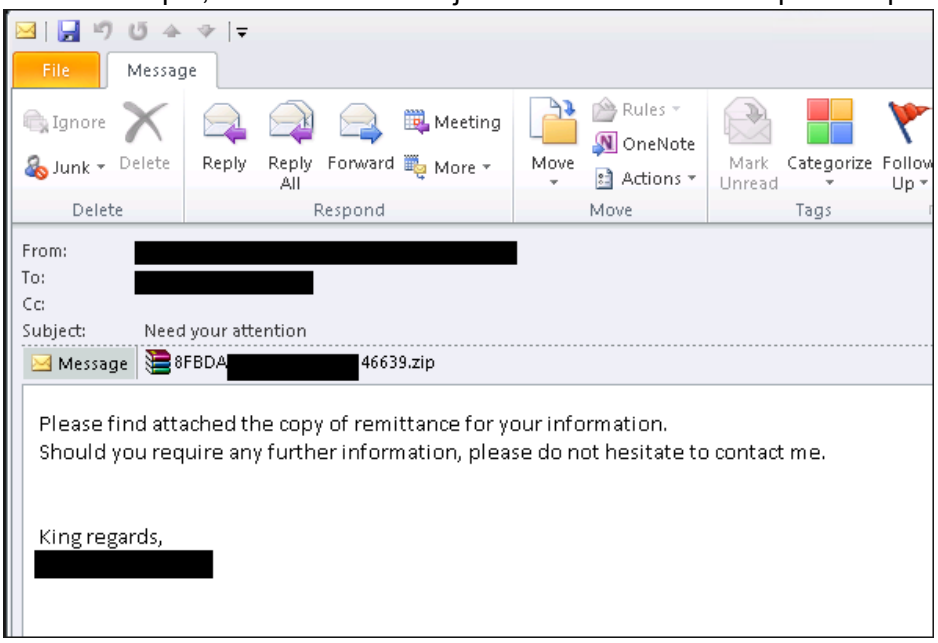
Despite antivirus software, e-mails containing malware may still occasionally land in your inbox. Currently the most dangerous are those containing ransomware, which prevents you from accessing your own data by encrypting it. In such cases, a “ransom” must be paid before the data is decrypted. An encryption trojan blocks both local files and those on linked network drives and servers. Within just a few minutes, it is capable of rendering all files on a corporate server unusable. Only greater staff awareness can help in such cases.

These features indicate a virus e-mail:

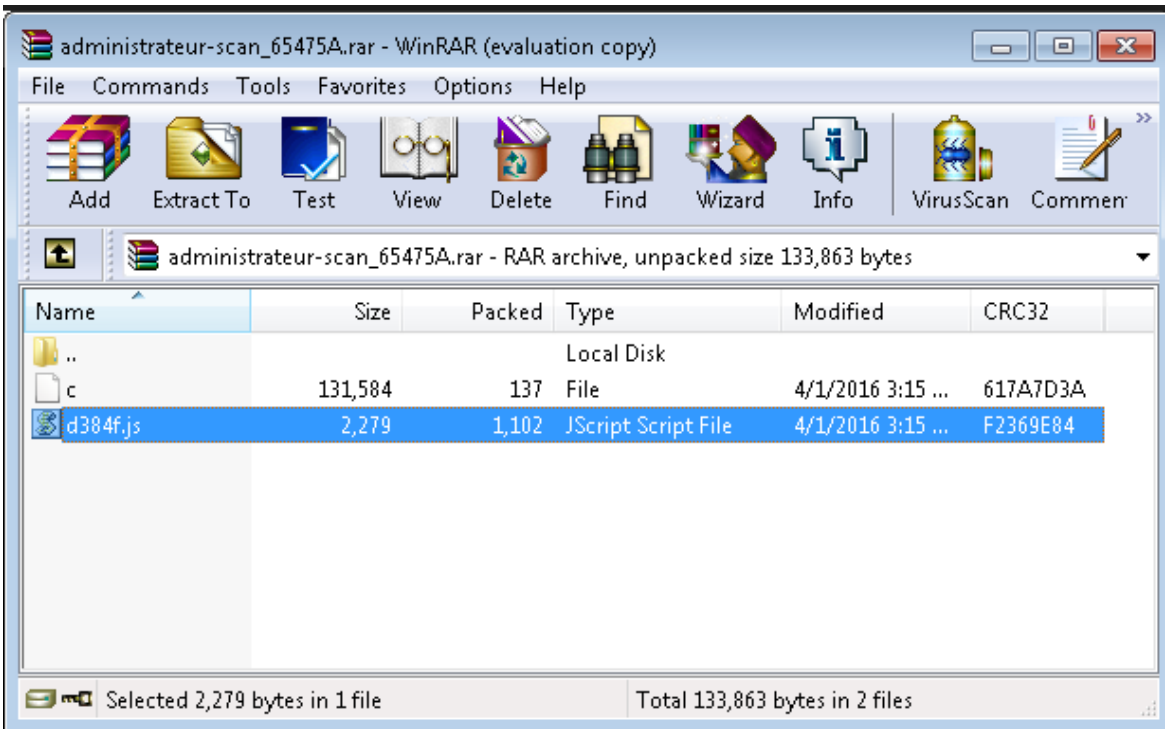
- Attachments containing executable files, such as those with the following extensions: .com, .chm, .cmd, .exe, .jar, .js, .ps1
- Attachments containing encrypted archives: .7z, .zip, .rar
- Attachments with double file extensions, such as: .pdf.zip, .doc.exe

If the file extension is not shown in File Explorer, leading you to believe that it is a PDF or Word document, you may be tempted to open it.

In this example, the “Nemucod” trojan is hidden as JavaScript in a zip file.



The zipped archive contains a JavaScript file.



If you double-click on this file, the malware connects to certain websites and downloads further malicious code.

```
function loadFile(path) {
  var objStream2 = WScript.CreateObject("ADODB.Stream");
  objStream2.type = 2;
  objStream2.charset = 437;
  objStream2.open();
  objStream2.loadFromFile(path);

  var fileContent = objStream2.ReadText;
  objStream2.close();

  return deobRound1(fileContent);
};

var fileContent = loadFile(tempFileName);
```

Protection Against Phishing and Malware

Treat your computer and mobile phone like a safe!

Passwords: Use a different password for each resource. This will limit the damage in the event of an attack, because the intruder will not be able to misuse any further services. You should also change your passwords at regular intervals. For greater security, they should consist of a mix of capital and lower-case letters, special characters and numbers.

E-mail addresses: Use several different e-mail addresses: The first one for important messages, and the second for registering with online services such as sales platforms, Facebook, Twitter, Google+ and other services.

Discretion: Less is often more. By not disclosing your data in the first place, you give potential attackers fewer opportunities to misuse it.

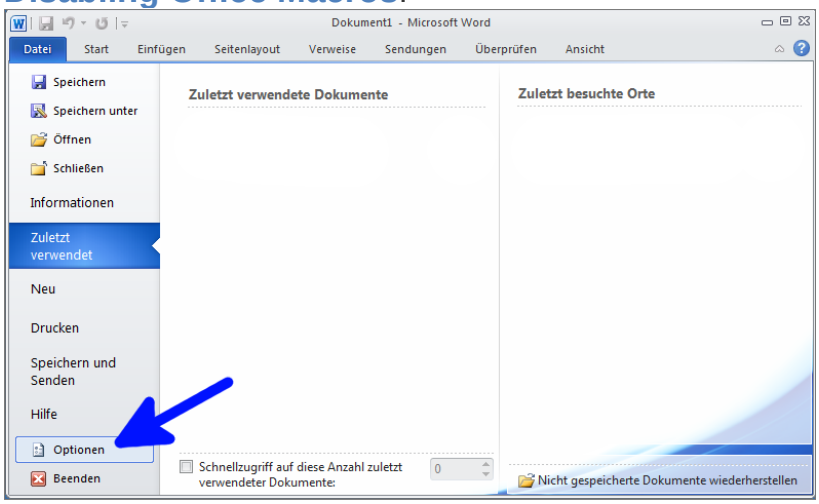
Additional information: “Real life” data such as your home and postal address or your personal telephone number should be given only where absolutely necessary for online services. Completing these fields is optional in many online forms.

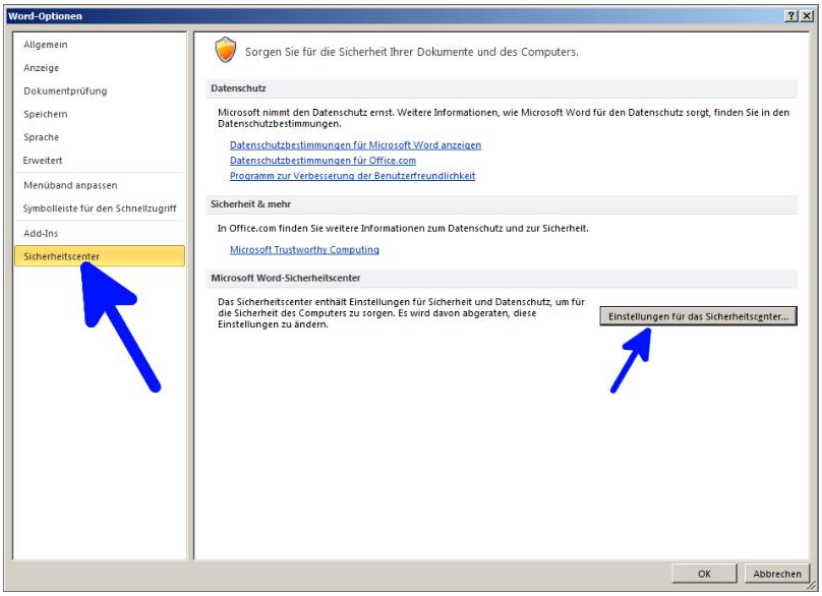
Encryption: There are many different ways in which you can encrypt your data when transmitting it online. Professional users often use the PGP encryption system, although this will be too complicated for most. However, since providers of online services such as Facebook and webmail are also aware of this problem, they often offer their users the option of at least working with relatively simply encrypted connections.

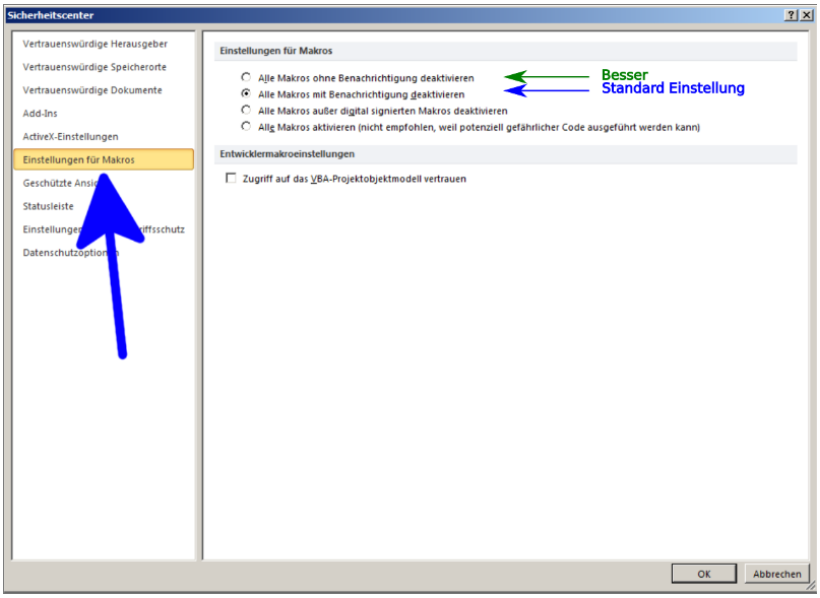
Authorization: Do not run software on your computer under administrator rights.
The default administrator account should not be used on an everyday basis. Instead, set up suitable user accounts – with restricted rights – for yourself and other users. This makes life more difficult for malware and hackers right from the start.

Microsoft Office macros – disable automatic execution: Macros are used in Excel to automate repeated sequences of tasks, and thus to save time and trouble. However, macros are also a good way of automating unwanted processes, such as malware downloads, making them a popular tool for hackers. Automatic macro execution is therefore disabled as standard in the most recent versions of Office.

Disabling Office Macros:







Further Information

Regulations on the Use of IT Tools

Regulations on the Use of IT Tools at the University of Zurich (RUITT)

PCs and MACs in Everyday Office Use

https://www.dsd.uzh.ch/dam/jcr:b2443ab4-f5c9-43a9-9fe9-23d0a7b10d95/UZH_DSD_Checkliste_Datenschutz_im_B%C3%BCroalltag_August2018_V2.pdf