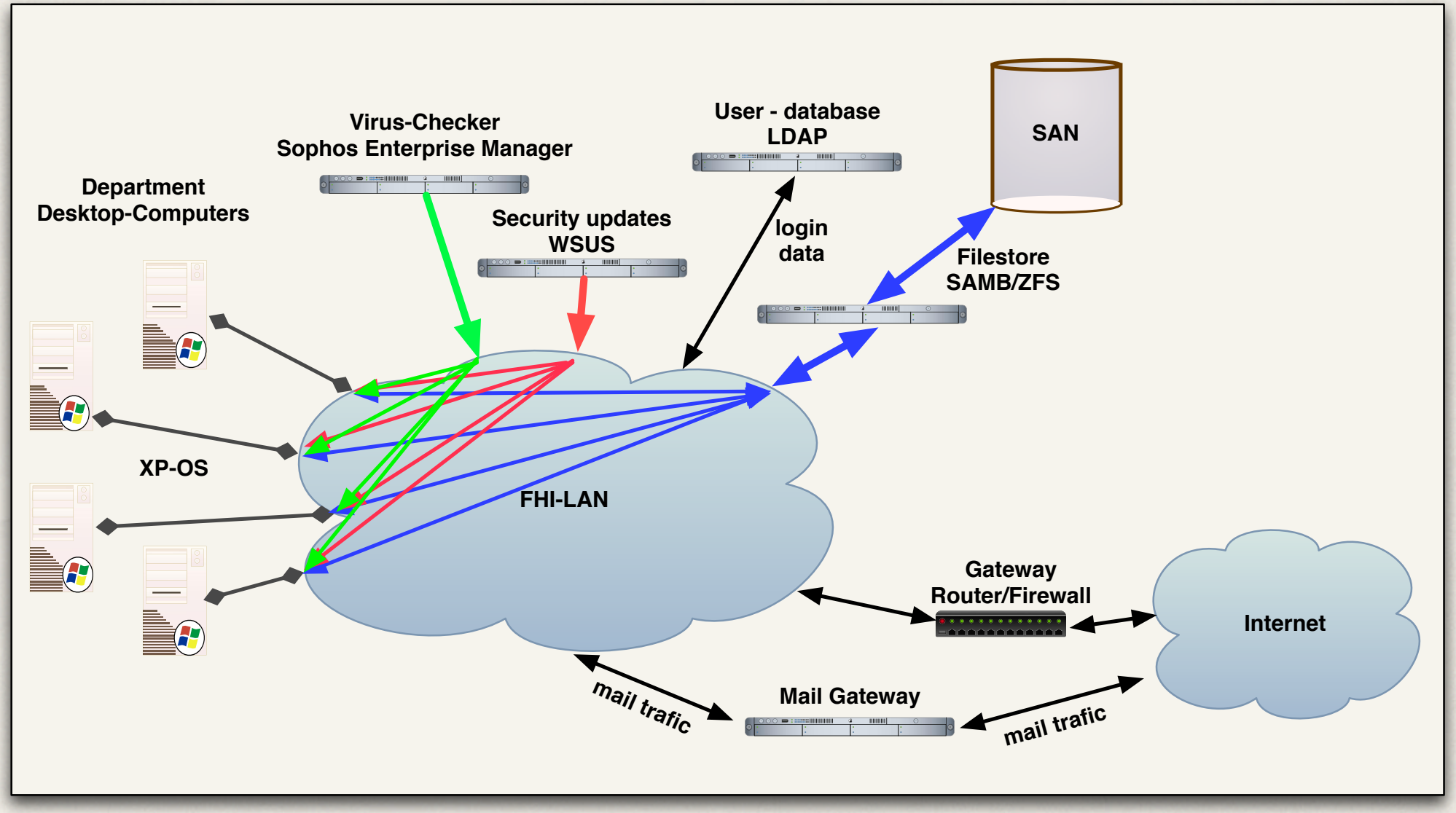
http://www.freewebs.com/sau83computersafety/

Computer Safety FHI (Dep. CP)

https://www.fhi-berlin.mpg.de/cp/ComputerSafetyDepCP.pdf

26. April 2010

Standard configuration personal computers



PP&B is security conscious

Because the number and intensity of break-ins (mostly on Windows computers) continue to increase, new security precautions will, no doubt, be instituted as necessary.

- Here are some of the measures we use to improve the safety and availability of the computing environment in the Fritz-Haber-Institut
  - **Long passwords.** Passwords should be at last 8 characters long.
  - **lock email known to contain virus; spam.** WhenPP&B knows of an alert about a specific virus being spread via email, messages from offending addresses are rejected. Mail sent from known spam sites is rejected and not delivered.
  - Campus wide the **virus-scanning software** is from Sophos. It scans files as well as provides antispyware protection. On administered computers the software ist always installed, running and will be updated.
  - A**uthenticate before sending mail if on non-secure network**. You must authenticate with a secure connection to the mail server to receive and send email. This requirement keeps people outside our network from using your computer to relay mail from and to other sites.
  - **Connect with secure (SSH) connection.** You cannot use telnet or rlogin to connect to a computer on the FHI-network because those two protocols are not secure. You must connect with an SSH (Secure SHell) connection to the host “ssh.rz-berlin.mpg.de”.
  - **Limit incoming traffic**. Self-administered machines cannot receive incoming traffic.

“best protection” (not a technical measure)

✳Secure your browser

Many labor under the dangerous misconception that only Internet Explorer is a problem. It's not the browser you need to be concerned about. Nor is it a matter of simply avoiding certain 'types' of sites. Known, legitimate websites are frequently being compromised and implanted with malicious **javascript** that foists malware onto visitors' computers. To ensure optimum browsing safety, the **best tip is to disable javascript** for all but the most essential of sites - such as your banking or regular ecommerce sites. Not only will you enjoy safer browsing, you'll be able to eliminate unwanted pop-ups as well.

In addition, please exercise discretion when browsing the internet and avoid unsecured and doubtful sites. Malicious hackers in particular corrupt websites advertising seemingly tempting offers or also pornographic oriented websites, the use of which is not permitted within the MPG in thre first place.

“best protection” (not a technical measure)

✶Take control of your E-Mail

Avoid opening email attachments received unexpectedly - no matter who appears to have sent it. Remember that most worms and trojan-laden spam try to spoof the sender's name. And make sure your email client isn't leaving you open to infection. Reading email in plain text offers important security benefits that more than offset the loss of pretty colored fonts.

✶Treat IM suspiciously

Instant Messaging is a frequent target of worms and trojans. Treat it just as you would email.

“best protection” (not a technical measure)

✶Avoid P2P and distributed filesharing

Torrent, Kazaa, Gnutella, Morpheus and at least a dozen other filesharing networks exist. Most are free. And all are rife with trojans, viruses, worms, adware, spyware, and every other form of malicious code imaginable. There's no such thing as safe anonymous filesharing. Avoid it like the plague.

✶Keep abreast of Internet scams

Torrent, Kazaa, Gnutella, Morpheus and at least a dozen other filesharing networks exist. Most are free. And all are rife with trojans, viruses, worms, adware, spyware, and every other form of malicious code imaginable. There's no such thing as safe anonymous filesharing. Avoid it like the plague.

“best protection” (not a technical measure)

✶Don’t fall victim to virus hoaxes

Dire sounding email spreading FUD (“Fear, Uncertainty and Doubt”) about non-existent threats serve only to spread needless alarm and may even cause you to delete perfectly legitimate files in response.

Von: "FHI" <iadmin@fhi-berlin.mpg.de>
Datum: 2. April 2010 13:45:15 MESZ
An: undisclosed-recipients:;
Betreff: Dear User
Antwort an: iiidepartment@gmail.com

Dear User,

During our regularly scheduled account maintenance and verification procedures, we have
detected a slight error in your account informations.

This might be due to either of the following reasons:

1. A recent change in your personal information (i.e. change of address).
2. Submitting invalid information during the initial sign up process.
3. An internal error within our processors.
4. Too many login for more than 24 hours

To verify you account with **fhi-berlin.mpg.de**, you must provide your username and password
within 24hrs for verification.

Please reply to update your account informations.
This alert relates to your email account only.

Impressum • © FHI
Webmaster: M.Wesemann.

```
ieve: CMU Sieve 2.2
Received: from divok.rz-berlin.mpg.de (localhost [127.0.0.1])
          by localhost (Postfix) with SMTP id D0843BCDB2;
          Fri,  2 Apr 2010 15:01:02 +0200 (CEST)
Received: from localhost.localdomain (divok.rz-berlin.mpg.de [141.14.131.15])
          by divok.rz-berlin.mpg.de (Postfix) with ESMTP id F1ABFBCDA3;
          Fri,  2 Apr 2010 15:01:00 +0200 (CEST)
Received: from unknown-host
          by divok with queue (Sophos PureMessage Version 5.401) id 2133622-1;
          Fri, 02 Apr 2010 12:49:50 GMT
X-Greylist: delayed 3201 seconds by postgrey-1.21 at divok; Fri, 02 Apr 2010 14:49:42 CEST
Received: from mail.freeweb.com.tw (mail.freeweb.com.tw [202.133.244.152])
          by divok.rz-berlin.mpg.de (Postfix) with ESMTP id 35A6ABCDA3;
          Fri,  2 Apr 2010 14:49:42 +0200 (CEST)
Received: from freeweb.com.tw (fw1.freeweb.com.tw [192.168.100.111])
          by mail.freeweb.com.tw (Postfix) with ESMTP id 776D87477F;
          Fri,  2 Apr 2010 19:04:09 +0800 (CST)
From: "FHI" <iadmin@fhi-berlin.mpg.de>
Reply-To: iiidepartment@gmail.com
Subject: Dear User
Date: Fri, 2 Apr 2010 19:47:38 +0800
Message-Id: <20100402114747.M4446@fhi-berlin.mpg.de>
X-Mailer: Open WebMail 2.51 20050228
X-OriginatingIP: 112.110.203.14 (iidc@freeweb.com.tw)
MIME-Version: 1.0
Content-Type: text/plain;
          charset=iso-8859-1
To: undisclosed-recipients:;
X-Seen-By: PP&B-Host divok
X-PMX-Version: 5.4.1.325704, Antispam-Engine: 2.6.0.325393, Antispam-Data: 2010.4.2.123921
X-PPB-Spam: Gauge=IIIIIIIII, Probability=9%
X-GMX-Antivirus: 0 (no virus found)
X-GMX-Antispam: 0 (Sender is in whitelist: %@fhi-berlin.mpg.de);
Detail=5D7Q89H36p4L00VTXC6D4q0N+AH0PUCnetdm6+jp8LGbv5ueRb0G1ImNQdo1ZfyjW58Ih
AhBpYZTHGo9yudGdEK/ni0PEVWnV1;
X-GMX-UID: xK7/DDoia2A6Le48MHQyn+4yOWhhakeT
```

“best protection” (not a technical measure)

✳Don’t use cracked software

Software cracking is the modification of software to remove or disable features which are considered undesirable by the person cracking the software, usually related to protection methods: copy protection, trial/demo version, serial number, hardware key, date checks, CD check or software annoyances like nag screens and adware.

The distribution and use of cracked copies is illegal. You should use only software which is licensed by the FHI

http://www.youtube.com/watch?v=O6U8cYBeA9A

Self administrated systems

If your computer is **self-administered**, you are responsible for providing much of the security that PP&B provides for PP&B-administered machines. Regularly **update the virus definition file**; **install software patches** as necessary; pay attention to information about **security holes** in the operating system you use. If PP&B or GNZ finds that a self-administered machine has been compromised, it will be disconnected from the network until the administrator has fixed the problem.

- One good way to protect yourself from spyware is to make sure that you never use your computer with administrator rights. All modern operating systems allow you to create multiple users and give them different rights on the system. Create an administrator user that you will use only when you want to install software and a user account for all other use. The user account should not have the right to install software. Of course you will also want to create an account that your kids or grandkids use. You don't want them erasing or moving your files.
- Autorun viruses generally creates viruses autorun.inf files in the root directory of the local drives and removable drives like USB Flash drives etc. Due to these virus autorun.inf files when you double click to open these drives the virus spreads and executes the code inside these autorun files.

Self administrated systems

Adobe Reader comes pre-installed on most computers. And even if you never use it, just the mere presence can leave your computer at risk. Vulnerabilities in Adobe Reader and Adobe Acrobat are the number one most common infection vector, bar none. Making sure you stay up-to-date with the latest version of Adobe products is imperative, but not foolproof. To use Adobe Reader (and Acrobat) safely, you need to make a few tweaks to its settings. Following are the must-make security changes you need to make in Adobe Reader and/or Adobe Acrobat.

Here's How:

1. Open Adobe Reader or Adobe Acrobat.

2. If you use Windows, click **Edit** and choose **Preferences**.
   If you use a Mac, click Adobe Reader (or Adobe Acrobat) and select **Preferences**.

3. **Prevent PDF files from launching programs:**
   From the left pane, select **Trust Manager**;
   Uncheck the box *Allow opening of non-PDF file attachments with external applications*.

4. **Prevent javascript from running in PDF files:**
   From the left pane, select **Javascript**;
   Uncheck the box *Enable Javascript*.

5. **Prevent PDF files from opening automatically on the Web:**
   From the left pane, select **Internet**;
   Uncheck the box *Display PDF in browser*.

6. Click OK and close the program.

personal computers used for measurement