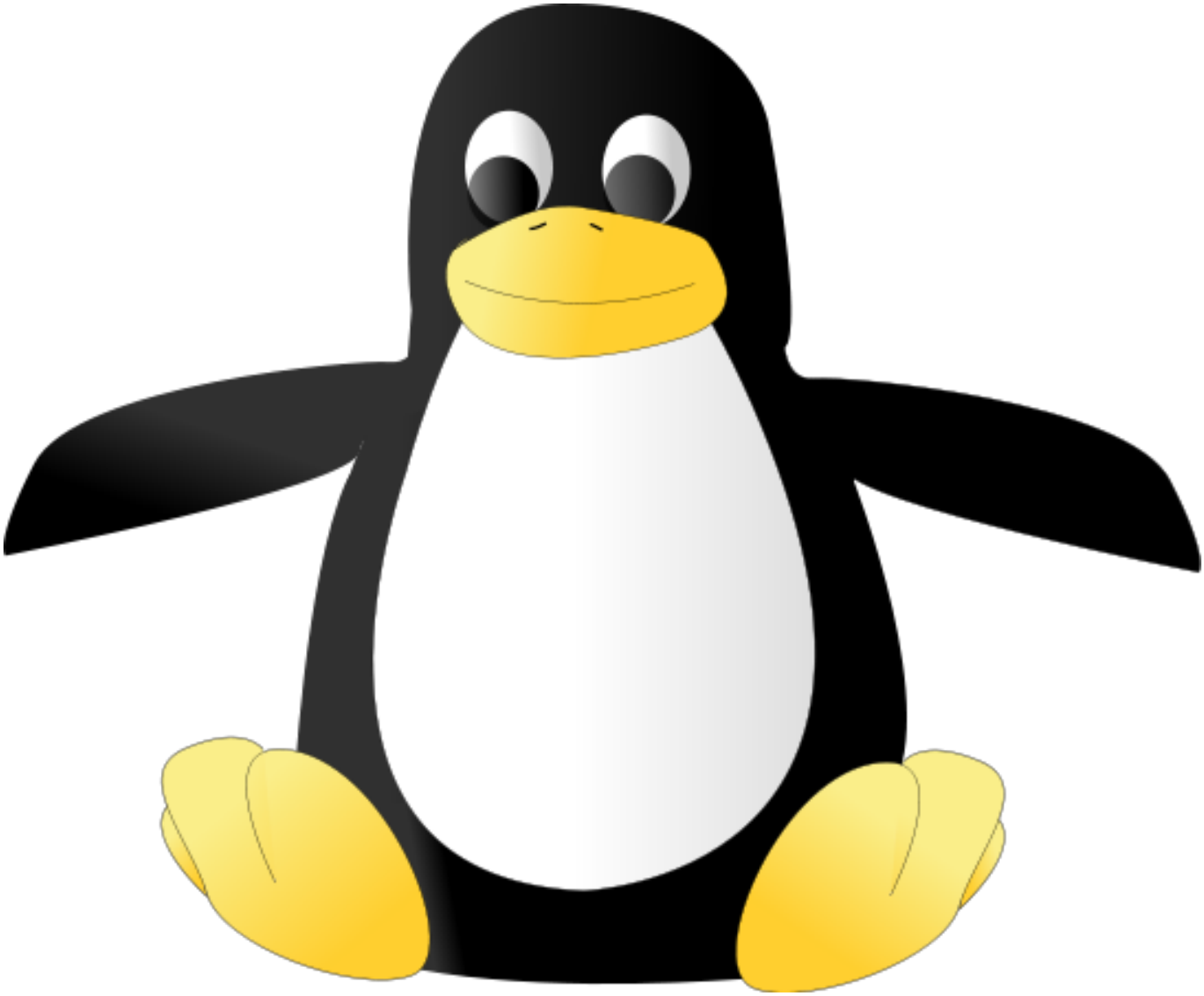
Malware

1. Malware [1] is a term for any software that is likely to do harm. This ranges from viruses that can destroy all your data to spyware and advertising cookies that cause annoying pop ups and automatically route your browser to sites you don't want to visit. If you let Malware [2] into the network you are being very anti-social!

2. For this reason network managers often disallow ordinary users from installing any software on the network. This can of course be a nuisance if you need to use some software that is not installed. There is always going to be a trade off between convenience and security.

3. Another reason why you may not be allowed to install software on a network is the issue of licensing [3]. For each installed copy of a piece of software, you need a license to prove that you legally have the right to use that software. Allowing anyone to install software will prevent the

network manager from keeping track of what is installed and whether they are all properly licensed.



4. Some software is licensed for free use [4]. A sensible policy is to use this as much as possible not only because it saves money, but also because it reduces the risk and costs associated with complex licensing conditions [5]. TLM adopts this policy and the Drupal environment in which you are working is free and open source software. A good place to get more free software applications is http://ninite.com/ [6].

5. Downloading software

We have to be careful when downloading software to our personal computers [7]. Things are not always as they appear. How do you know that the ninite web site has not packaged up malware to look like useful applications?

The answer is that you don't. However for a major site that has been around a while it is unlikely. One way to check this is from the site's Google rank [8]. Google rank tells us how important a site is in terms of the number of people connecting to it. It is very unlikely that a site with a Google rank of above 5/10 is a malware site because it would get closed down long before it reached this status. If a malware site does have a reasonable Google ranking and you search for it you are likely to get a lot of references to its bad effects. Try searching for Spysherriff [9] and you will see that this was a well-known deliberately misleading scam. In all of these issues we are considering risk - nothing is ever 100% safe. If you want 100% safe, don't get out of bed in the morning! Believing anything can be made 100% safe is probably the biggest risk! It is better to understand that there are risks and be cautious but not over-p [10]aranoid [10] :-)

6. **Checking a site's Google Rank**

To check a site's Google Rank go to the web site here [11]. Enter the web address of the site in the box starting http:\\ eg type in ninite.com. Copy the anti-bot letters and click verify now. At the time of writing it returns 6/10 (it might increase if the site becomes more popular). If you find a site with 0/10 it is probably very new or very obscure. Be careful, it could be a scam!

7. Malware is mostly computer programs

Computer programs do things on computers. If the intention is to do bad things then the program is

(function(i,s,o,g,r,a,m){i['GoogleAnalyticsObject']=r;i[r]=i[r]||function(){ (i[r].q=i[r].q||[]).push(arguments)},i[r].l=1*new Date();a=s.createElement(o), m=s.getElementsByTagName(o)[0];a.async=1;a.src=g;m.parentNode.insertBefore(a,m) })(window,document,'script','//www.google-analytics.com/analytics.js','ga'); ga('create', 'UA-46896377-2', 'auto'); ga('send', 'pageview');

malware. Simple really :-)

In general computer programs are written specifically for particular computer operating systems so malware that affects one type of computer is unlikely to affect others. Microsoft Windows [12] is by far the biggest target of malware so the first consideration is do I really need to use Windows? At TLM we made a decision not to. We do things like internet banking and we can reduce risk by not using the biggest target for malware on our computers. Of course that also means we can't run a lot of popular software but there are free versions of just about all major tools. You can do the entire INGOT qualifications suite without ever needing to buy software licenses. This in turn saves us money because we don't have to pay for software licenses or manage license administration, we don't need to buy anti-virus software or slow down our computers running it. So far we can pass on those saving to customers and make our business more financially competitive. Of course having the confidence to do this requires learning and this demonstrates why Lifelong Learning in the field of technology is important. It will save you money! :-).

Source URL: https://theingots.org/community/malware#comment-0

Links
[1] http://en.wikipedia.org/wiki/Malware
[2] http://www.youtube.com/watch?v=KH3FFVrxL5k
[3] http://www.wisegeek.com/what-is-software-licensing.htm
[4] http://en.wikipedia.org/wiki/Free_software_licence
[5] http://www.pcpro.co.uk/blogs/2009/10/08/the-shame-of-microsofts-media-center-eula/
[6] http://ninite.com/
[7] http://news.cnet.com/8301-27080_3-20003453-245.html
[8] http://en.wikipedia.org/wiki/PageRank
[9] http://www.google.co.uk/search?aq=f&sourceid=chrome&client=ubuntu&channel=cs&ie=UTF-8&q=Spysherriff
[10] http://en.wiktionary.org/wiki/paranoid
[11] http://www.prchecker.info/check_page_rank.php
[12] http://windows.about.com/b/2009/12/15/2010-prediction-malware-will-target-windows-7.htm