

## This fact sheet describes some common email hoaxes and how to avoid falling victim to a scam.

Despite the best efforts of ITS and our security software, small numbers of hoax emails continue to be received at UWS. Unfortunately, your being fooled by a hoax can cause large problems to the University, and may even result in your personal financial details being provided to criminals.

No software or system can guarantee 100% protection, which means we need to be aware of the problem, and to “**think before we click**”.

*Personal awareness is one of the best defences against hoaxes, and is your final defence against criminals seeking your financial or personal information.*

**If you are concerned about the contents of a message, contact ITS (ext 5111) for advice.**

Hoax emails may be merely annoying, such as chain emails, urban myths and fake virus warnings, or they may be malicious.

Malicious hoaxes may be designed to convince you to enter your personal details into a website that appears legitimate, but isn't. Once your details are provided, they will be used by scammers and criminals.

**Never reply to these emails. Suspect email can be forwarded to: [spam@uws.edu.au](mailto:spam@uws.edu.au)**

### Password requests

Your password is your key to your online identity. Don't disclose it to others, even when sent an official looking email. UWS does not ask users for their password.

### Bank account scams

These scams are particularly effective if you have an account with the bank that has apparently sent the email. They appear to come from a legitimate financial institution, and tell you to follow a link in the email and enter your password details.

Follow the link, and you'll see what appears to be the institution's web site. Everything seems to be above board. You enter your details, and money starts leaving your account. Sadly, you didn't notice that the web page address didn't actually belong to your bank.

**NEVER** follow email links to banking websites, even if the address appears to be valid. **ALWAYS** manually enter your bank's web address into your web browser's address bar. It's trivial for criminals to create fake websites and to fake “from” email addresses.

### Urban myths

Urban myth messages are often willingly forwarded by well meaning recipients. It's best not to forward them at all, but if you feel you must, do some research to check if the story is true, and/or current. Googling the story can provide more information.

**A good source for urban myth busting is <http://www.snopes.com>.**

### “Nigerian” scam

These days this scam originates from many countries.

Someone needs your help to access large sums of money, which have been mysteriously tied up. In return for your assistance, you will be showered in riches. You may need to pay a few “small” fees to help, but the fees are small change in comparison to the supposed rewards on offer. The fees won’t stop, and the reward will never arrive.

Hmmm – there’s a reason these claims seem too good to be true – they aren’t! Unfortunately our own greed makes us prey for these scammers.

### Trojans

Seemingly innocuous attachments or websites that are up to no good. Opening the attachment or visiting the website secretly installs the trojan on your computer, which does things like stealing passwords and account details, joining your computer to a zombie botnet (providing criminals with free processing for their activities), or sending emails in your name.

One recently compromised UWS email account generated over 120,000 outbound messages, and the user experienced weeks of frustration as message bounces and complaints were returned. Worse still, such compromises can lead to University mail servers being blacklisted worldwide, affecting the entire University’s ability to communicate with the outside world.

Always treat attachments with care and don’t follow unexpected links in emails.

### Chain emails

Don’t send them. Ever. Please.

### Fake virus warnings

It’s an old joke in IT that fake virus emails cause more problems than real viruses, as IT departments struggle to defuse panic from the incorrect information and cope with the massive increase in support requests – especially when the warnings exhort users to delete vital operating system files. Often someone authoritative (such as a representative of Microsoft or Norton) is quoted in these warnings to give the message legitimacy, however, if the person exists, they didn’t make the comments.

Some classic hoaxes have included “It takes guts to say Jesus”, “Budweiser Frogs” and the infamous “Good Times”.

Ignore the recommendation of the email to resend the virus warning to all your friends. Ignore the excessive exclamation marks!!!!!! Use the web to check if the warning appears legitimate, and if it does, **forward the email to the IT Service Desk for investigation.**

If necessary, ITS will take pro-active measures to prevent problems and will issue a formal warning to all staff.

Many antivirus companies have information about hoaxes and/or databases of genuine viruses on their websites.

<http://www.sophos.com/security/hoaxes/>

### What to do if affected

**If you think you may have inadvertently followed a link in a hoax email, please contact the ITS Service Desk for further advice – ext 5111, or email [its servicedesk@uws.edu.au](mailto:its servicedesk@uws.edu.au).**