



# Risk Management Tips

## Using Email Securely

Many computers may already have safeguards in place to prevent viruses and other malicious software (malware) from reaching your inbox. Nevertheless, it is virtually impossible to stop them completely. Occasionally, email with viruses can get past the protective perimeter, leaving you as the last line of defense. How you handle emails with attachments or embedded links can determine whether your PC becomes infected with a virus or not.

If you do get a virus, it could result in anything from a minor inconvenience while the virus is removed from your PC to a complete shutdown of your camp's computer network if the virus spreads rapidly throughout the system. A few simple steps can protect your PC assets from potential harm.

### How best to handle suspicious emails

#### *Attachments*

Consider the following points when you receive an email with an attachment:

- Do you know the sender?
- If not, be especially suspicious. Never open any files or macros attached to an email from an unknown or untrustworthy source.
- Was it sent from a camp employee or from an outside entity?
- Even if it was sent by a staff member, it doesn't automatically mean it is safe. The email could be an attempt by the virus to spread.
- Are you expecting the attachment?
- If an attachment is suspicious or you have any doubt, consult with your IT specialist or just delete it.
- Do not forward the message to others until you are completely sure it is not infected with a virus.

#### *Embedded links*

An embedded link is simply a link to a website in the content of an email. Sometimes you will see the full address such as <http://www.samplename.com> or you may only see [Company Website](#). In either case, do not click on links contained in an email without considering the points noted above in the "Attachments" section. The link could direct you to a website whereby simply going to it, you will download a virus or other form of malware.



## *Spam*

Spam is unsolicited email, usually sent indiscriminately in bulk to a large number of people. Spam often touts an unscrupulous company's product or service or tries to entice recipients into a scam or visiting a fraudulent website. Spam usually contains a false "from" address, otherwise known as a spoofed address. It is often sent from botnets, which are unknowingly virus-infected machines in people's homes and workplaces.

Tips for dealing with spam:

- Do not reply to spam emails, as this confirms to the sender that the email address exists.
- Avoid opening spam emails. If you do, ensure you do not download any HTML content in the email.
- Be wary of giving out your email address. If you do, ensure you ask that your email address is not shared with other companies.
- Install spam filtering software on your machine, or use an email account set with a high anti-spam level. This will minimize the amount of spam you receive.

---

If you have a safety or risk management question or a suggestion for a topic, please contact Markel's Risk Management Department at [safety1st@markelcorp.com](mailto:safety1st@markelcorp.com).