UK BIM Alliance – BIM Security Guidance

Appropriate Use of Email

Title of guidance:	*Appropriate use of email.*
Author:	*Rick Hartwig*
Company:	*The Institute of Engineering and Technology*
Email:	*RHartwig@theiet.org*
Objective of guidance:	*Support adoption strategies for secure email.*

Abbreviations/acronyms	**Full name**
CDE	*Common data environment*

Relevant/referenced sources	
PAS 1192-2: 2013	*Specification for information management for the capital/delivery phase of construction projects using building information modelling*

Keywords:	Email, trojans, phishing, malicious emails, password, inbox, employee, behaviour, links, attachments, sensitive information, CDE, Common Data Environment

Briefing note text

We seem to have a love/hate relationship with our email 'inbox'. At times it is relentless and with the advent of hand held devices it has become something of a nervous tic as we check the inbox throughout the day, when in meetings and even at home after hours! Yet it is marvellous communication tool and business certainly could not operate without at the present time.

For a system that's has become so mundane in personal and business life, it can be fraught with risk which is why we do need to be proactive about implementing strategies to ensure the 'appropriate use of email' in the context of cyber security. Email security is necessary for both individual and business email accounts, and there are multiple measures organizations can take to enhance email security.

Following the guidelines can help lead to a reduction in the risk run by companies:

1. Protect System Infrastructure

   Techniques such as trojans, phishing emails or linking to malicious websites conspire to steal sensitive business and personal information. Make sure internal corporate emails are double checked as if a PC becomes infected with malware, it may be sending malicious emails without the users knowledge. This can be prevented by acquiring a service that stops malware from entering your inbox.

   To ensure there is no loss of private information encrypt out going emails. Require employees to use strong passwords and mandate password changes periodically. Implement security best practices for 'Bring Own Device' if your company allows employees to access corporate email via webmail or personal devices.

2. Email attachments

   E-mail attachments consume inordinate amounts of e-mail server space and network bandwidth and are frequently the culprits behind virus outbreaks—but they're often the easiest way to transfer information. Word Docs, Excel and PDF files are the most common attack files used for malware.

   Attachments with macros are especially sensitive. Users are more likely to click on a link from someone we know versus someone we don't know.

As a general rule of thumb, emails should be size restricted (for example: 10MB). This is because some emails may not deliver attachments this large, and the sender may not always be notified that their email never sent.

3. Employee Behaviours

   Establish an email policy and train all employees so that appropriate behaviours are encouraged, such as:

   - Being aware of email security risks and how to avoid falling victim to phishing attacks
   - Taking caution over unexpected attachments in an unfamiliar email, if in doubt don't open them
   - Be wary of hyperlinks in email messages

4. Interaction with common data environments

   The common data environment (CDE) is defined as a *single source of information for any given project, used to collect, manage and disseminate all relevant project documents for multi-disciplinary teams in a managed process*[1]

   It is therefore important that email is used in consideration of this, particularly when it is the means of conveying project information/files which should in reality be held on the CDE. To help efficient and managed release of information it is suggested that email attachments are minimised and instead emails contain links to files held on the CDE. This will assist baseline security in that individuals should only be able to access the files linked via email if they have permissioned access to the CDE.

   In addition many CDE's have the ability to 'notify' recipients about files held on the CDE, further minimising the need for email attachments.

[1] PAS 1192-2:2013. Specification for information management for the capital/delivery phase of construction projects using building information modelling