FAIRDINKUM

LEVERAGING INNOVATION WITH TECHNOLOGY

Employee Email Safety Guidelines

Attack Type: Phishing

Phishing is a tactic used to gain personal information (Credit card info, SS#, Passwords and Usernames) via spam emails. These emails are crafted to look as though they came from your network administrator, Credit Card Company, bank or other common sources such as Apple, IRS, etc… and will often link to websites where you are asked to input personal data.

Defense: Phishing

1. Most agencies will never ask you to input your personal information through email based links. If you believe the email received is legitimate the best course of action is not to click on the link within the email but to login in to the online account in question directly from a web browser. You will often be alerted to any issues once successfully logged in.
2. When an email is received with embedded links you can hover your mouse pointer over the link without clicking and the true website link will be revealed. Often the links in emails are edited to appear legitimate but once hovered over you will see they do not point to the business supposedly sending the email.

Attack Type: Malicious Attachment

Spam sent containing malicious attachments is another common attack. This attack varies in the method of file acquisition and our spam filters block most however there are two methods used most often because we cannot block them due to the fact they are used in legitimate file exchanges, they prey on these legitimate methods and file types. Most commonly the email will contain a download link in the form of a link to a document or invoice but will in reality be a malicious file. The second most common type of attachment will be in the form of a .Zip file attachment.

Defense: Malicious Attachment

1. Anytime you receive an unexpected email containing an attachment or download link you should forward it to Fairdinkum for review.
2. You should hover your mouse pointer over download links without clicking and compare the written link to the true link, if they differ it is most likely a dangerous download.
3. Zip attached files from unknown sources should never be downloaded. If downloaded and unzipped Fairdinkum should be notified immediately
4. File types stored inside Zip files even from known senders that should be avoided are .HTM, .EXE and .HTML. It is possibly that a known sender's email account has been compromised and the attachments sent malicious.

Attack Type: Malicious Online Sharing Files

With the rise in use of online sharing and syncing software (Dropbox, Google Drive, Box.net, OneDrive, Etc…) these legitimate services have begun to be used as a method of malicious file transfer. Unlike the previously mentioned malicious attachment attacks the links to the online sharing sites will appear and will be legitimate links, also our spam filters will not be able to scan the contents of those links to determine if the files being shared are malicious. Over time the services themselves analyze high traffic links and shut them down independently but that will usually take a few hours.

Defense: Malicious Online Sharing Files

1. Do not click on online sharing links from unknown or unexpected senders.
2. If a file is downloaded it should not be run (double-clicked) if it matches one of the below file extensions: .EXE, .HTM, .HTML, .BAT, .COM, .SCR, .CMD
3. If a file is downloaded and then double clicked after downloaded, the PC should be turned off and Fairdinkum should be alerted immediately.