Ransomware attacks globally have risen 350% and they cost businesses more than £70 billion per year worldwide.

95% of all cyber-attacks are caused by a successful phishing email. Approximately 6 million potentially malicious emails were blocked by University systems in 2020.

92% of malware is delivered by email. It is estimated that there were over a billion malware infections worldwide in the past year, and this is increasing year on year.

All cybercrime is up 600%. Social Engineering based cybercrime saw a 300% increase in 2020 mainly due to COVID-19 related scams and the increase in home working.

Guidance: Review our Social Engineering guidance and home working guidance, advice from the National Cyber Security Centre and complete your Information Security Awareness Training.

Always report suspicious emails to the IT Service Desk – servicedesk@abdn.ac.uk, and be aware of telephone or SMS based attacks.

Guidance: Never click links or open attachments in suspicious or unsolicited emails. Review information security advice on Toolkit and complete your Information Security Awareness Training.

If you require further information please contact the Information Security Team email: servicedesk@abdn.ac.uk
The University can be fined for failing to handle personal data properly. BA were fined £20 million by the Information Commissioner (ICO) for a data breach. This is the largest fine the ICO has imposed for a personal data breach. If you are unsure about how to handle personal data see our guidance or contact the Information Governance Team.

Over 12,000 personal data breaches are reported annually to the Information Commissioner (ICO). They happen at the University too. We can all take easy steps to avoid the most common type of breach – email misdirection.

If you are engaging a supplier to handle University data you MUST consider undertaking a Supplier Cyber and Data Assessment (SCDA). This is to ensure that the suppliers we do business with offer sufficient safeguards for personal and University data. If the supplier will be paid less than £10,000 use a Standard Assessment. Higher value contracts need an Enhanced Assessment.

Individuals have the right to request both their own personal data from the University, as well as other non-personal information.

In 2020 527 requests were received by the University. These requests must be responded to either within one calendar month or 20 working days.

GUIDANCE: If you think that a personal data breach has occurred, please contact the Information Governance Team at dpa@abdn.ac.uk as soon as possible.

GUIDANCE: If you are asked to help respond to a request, please respond promptly, to ensure the deadline can be met.


ACTION POINT: You can switch off auto Complete. This hugely reduces the chance of emails being sent to the wrong recipient. Please read our guidance on how to turn off AutoComplete.