Top tips to deter cybercrime

- The best protection against cybercrime is a strong password – use one with a mixture of upper- and lower-case letters, numbers, and special characters. Make sure you have a different password for all email and social media accounts, as well as any internet-enabled devices (such as smart speakers).
- Enable two-factor authentication where possible – this involves an extra layer of security, such as entering a unique code sent via text, to ensure only someone with legitimate reason can access the system.
- Conduct a virtual walk-around your processes to check basic security measures such as:
  - Ensuring anti-virus software is installed and enabled across all devices
  - Reviewing your social media privacy settings
  - Enabling auto-updates across devices so that you're always working on the latest, most-secure versions of software
- Backing up work can be one of the easiest ways to avoid data loss issues in your business – investigate an auto-backup service that uses a cloud-based system like Microsoft OneNote or Google Docs, or manually back-up your work at the end of every day.
- When browsing or shopping online, look for the green padlock in the address bar – this means the website you're visiting is safe and unlikely to cause issues like virus transfer.
- Criminals are using emails to 'phish' individuals – trick them into sharing personal or financial data. If you don't recognise the email address, or the request seems unusual, delete it – don't reply and don't click any links.

Business Inspired Growth
York & North Yorkshire GROWTH HUB

NYP20-0054