DIGITAL CRIME

FIRST PRINCIPLE

norfolk.police.uk/firstprinciple
suffolk.police.uk/firstprinciple

Top Tips

- Any crime can have a digital element.
- Anyone can be a victim of digital crime.
- Examples of online crime can include harassment, blackmail, fraud, youth produced sexual imagery and grooming.
- Resources available that can provide online safety advice and help to victims of crime:

  www.getsafeonline.org
  www.saferinternet.org.uk
  www.actionfraud.police.uk
  www.nsvictimcare.org

- Do Not use unsecured Wi-Fi networks for banking.
- Check for signs of Phishing emails, DO NOT open emails you are suspicious of.

PREVENT CRIME

PROTECT COMMUNITIES

NORFOLK CONSTABULARY
Our Priority is You

SUFFOLK CONSTABULARY

Digital Crime refers to a variety of crimes carried out online; using the internet through computers, laptops, games consoles, internet-enabled televisions, and smart phones.

Please note the advice and risks raised on this leaflet are not the only factors to consider. Always do your own research whether it is for personal or business needs.

Digital Security Advice

- Keep personal information private. Do not hand out passwords, passcodes, bank details, financial information, etc.
- Keep security and anti-virus software current.
- Be aware of suspicious emails, texts or phone calls – note bad grammar and spelling or low-quality images and logos; genuine senders will address you by your name.
- Do not reply or click on emails from businesses or individuals you do not know – they maybe spam emails.
- Use separate passwords on all accounts you use. Make your password strong - make it as long as possible, include upper and lower-case letters, include numbers and symbols.
- Make sure all devices are set up with a passcode or PIN.

Digital Social Media Advice

- Have separate passwords on all social media accounts. If your accounts are jeopardised, change all passwords. Better still, delete accounts and create new ones.
- Keep personal information confidential.
- Know and manage your friends. Only accept and communicate with verified friends.
- Protect your reputation on social networks, think twice before posting.
- Know what action to take. If you believe someone is harassing or threatening you, remove them from your friends list, block them and report them to the site administrator.
- Learn about and use the privacy and security settings on social networks.
- Delete links in email, tweets, posts, messages and online advertising that are suspicious.

Two-Step Authentication

- Is a method of confirming a user's claimed identity (often used by banks) utilising something known to both parties i.e. a password and a second method other than something they have, or something they are. An example of a second step is the user repeating back something that was sent to them through an out-of-band mechanism i.e. a code sent by SMS text message.

Public Wi-Fi Security Advice

- Unless you are using a secure webpage, do not send or receive private information.
- Do not share account information with others.
- Do not use unsecured Wi-Fi Networks for banking.

- Where possible use commercial hotspot providers such as BT Open Zone.

Online Dating

- Pick a username that cannot be associated with you.
- Keep personal information private. Stay in control by not including mobile numbers and other contact details on your profile.
- Be aware of the types of people that could attempt to convince, or pressure you to give personal, or financial information.
- Do research on people you are speaking to and take your time.
- Do not share intimate images of yourself with anyone, once they are sent they are online forever and authorities have no ability to retrieve these.

Hacking/Unauthorised Access

- If you think someone has access that shouldn't have, immediately regain access to accounts using the 'Forgotten Password' option – use a strong password and one that could not easily be guessed.
- Consider what access the individual already has and limit ability to further access.
- Change Wi-Fi password/key on network access points (if applicable).
- Remove devices from accounts through your account settings (if applicable).
- Consider joint devices and remove accounts shared with partners, ex-partners, family members you no longer wish to share access with.

NB. Contact your internet service provider for advice on all of the above

Harassment/Blackmail/Unwanted Contact

- Do not respond, do not accept any messages or friend requests from strangers.
- Take screenshots if suspect activity occurs.
- Save any call log files and relevant emails, messages, if suspect activity occurs.
- Record relevant suspicious URLs and IP addresses if identified.
- Block sender content has been screen shot, saved etc.
- Do not meet any demands, regardless of the threat and contact police immediately.

Sexual Offences Involving Children

- In the eyes of the law a child is any person under the age of 18.

- Stop and think about conversations you might be having online; is this with someone under 18? Is this appropriate?
- Never ask for a photo from anyone who you suspect might be under 18 – even if they say they are over 18.
- Do not accept friend requests from unknown users that you suspect may be under 18.
- If you receive an image of a child – delete the image and contact the Police immediately; call 999 if you believe a child to be in any immediate danger.
- Parents – be aware of what your child is doing online, monitor their social media, be aware of locked or hidden folders. Have open and honest conversations around who your child is talking to online, check their photo gallery, be aware of parental control features on smart devices.

First Principle: Related links

Check out all of our Crime Prevention information using the following links or by using the QR code to take you to the First Principle Pages Alternatively go to our website at https://www.suffolk.police.uk/ and look in the 1st Principle A-Z of Crime Prevention.

Allotment Security
Anti-Social Behaviour
ATM Security
Beach Hut Security
Boat Security
Building Site Security
Business Security
Caravan Security
Caravan Storage
Card Security
Catalytic Converters
Church Security
Cold Callers
Commercial CCTV
Counterfeit Banknotes
County Lines Advice for Landlords
Cyber Crime
Cycle Security
Dangerous Dogs
Dog Fouling
Dog Theft
Domestic CCTV
Domestic Violence
Farm Security
Fraud Prevention
Grooming
Hate Crime
Heating Oil
Home Improvements
Home Security
Home Security for Tenants
Horses and Stables
Keyless Vehicles
Key Safe Security
Lock Snapping
Mopeds and Scooters
Motorcycle Security
Neighbour Disputes
Occupiers Liability
Personal Security
Power Tool Security
Products Brochure
Rural Crime
Security Alarms
Sheds and Garages

Social Media
Social Media for Parents
Suspicious Behaviour
Shoplifting
Taxi Driver Safety
Vehicle Security
Windows and Doors

Other Links you might find helpful

Ask the Police
Secured by Design
Sold Secure

Crimestoppers
0800 555 111

Victim Care
0300 303 3705