

# CYBER CRIME



FIRST PRINCIPLE

[norfolk.police.uk/firstprinciple](https://norfolk.police.uk/firstprinciple)

[suffolk.police.uk/firstprinciple](https://suffolk.police.uk/firstprinciple)



**NORFOLK**  
CONSTABULARY  
*Our Priority is You*



**SUFFOLK**  
CONSTABULARY

## Key Points to Consider

- Cybercrime can be explained by breaking it down into two terms; cyber enabled and cyber dependent.
- Cyber enabled crime is where existing and traditional crimes are transformed in scale or form by use of the internet. E.g. Harassment, Blackmail, Youth Produced Sexual imagery.
- Cyber dependent crime is where the crime can only be committed online with the use of technology. E.g. Hacking, Denial of Service Attacks, Ransomware

**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.**



## Backing up your data

- Identify what needs to be backed up. Test that your back-ups can be restored. This can form part of your 'Disaster recovery plan' which can be implemented if you encounter a breach.

## Work devices

- Smartphones and tablets are now supplied to employees and used outside the safety of the business networks.
- Make sure all devices are set up with a passcode or PIN.
- Set up the devices so if lost or stolen you can track and/or remotely wipe. Inform users of devices to not send sensitive information whilst connected to public WIFI.

## Malware

- Install approved antivirus software on all devices.
- Keep software up to date on all devices. If there is an 'auto update' option make use of this.
- Consider disabling ports on devices to prevent external threats.
- Ensure your firewall is switched on. This will create a buffer zone between your network and the internet.

## Phishing attacks

- Check for signs of phishing within the emails
- Bad grammar and spelling
- Low quality images and logos
- The sender email address
- The text being added as a photo rather than written text
- If there is any concern that a breach has occurred run a scan as soon as possible and isolate from the network

## How do I protect myself?

In today's world we use the internet in day to day life for shopping, banking, paying bills and communicating. The internet allows us to stay connected at anytime, anywhere HOWEVER there are risks to be aware of.



## Public WIFI

- Unless you are using a secure web page do not send or receive private information.
- Where possible use commercial hotspot providers such as BT Open Zone.

## Internet Banking

- Do not use unsecured Wi-Fi networks for banking.
- Keep your banking app updated
- Be aware of emails, texts or even phone calls claiming to be from your bank. Fraudsters will tell you there is an issue with your account and request log in or other confidential and personal information. A bank will never request this information.

### Identity theft

- Do not share account information with others.
- Where possible arrange for paperless bills and statements.
- Have an effective and up to date antivirus software running.

### Ransomware

- Do not reply or click on links from spam emails, businesses or individuals you do not know or recognise.
- Regularly back up your data on an external hard drive.
- Ensure you have up to date antivirus system.

### Online abuse

- Keep your social media accounts private and locked down
- Check privacy settings regularly, especially when apps are updated.
- Make use of the block and reporting functions available
- Do not reply.
- If the abuse is serious enough to report to the police try to keep

emails, messages and posts as evidence.

### Revenge Porn

- Do not send indecent images of yourself even when legal to do so.
- Remember that once an image or video is sent you lose control
- If you are a victim report it to the Police.

### 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 getting to know people online.

### Passwords

- Use a separate password for every account you have.
- Make your password strong
  - *Make it as long as possible*
  - *Include upper and lower case letters*
  - *Include numbers and symbols*
- Regularly change your passwords.
- Do not recycle passwords.

# First Principle: Related links

---

## Ask the Police

Official Police Resource. The Ask the Police website provides you with information on a wide range of non-emergency policing matters.

[askthe.police.uk](http://askthe.police.uk)

## Secured by Design

Official UK Police initiative that combines the principles of 'designing out crime' with physical security.

[securedbydesign.com](http://securedbydesign.com)

## Sold Secure

Dedicated to reducing the risk of crime by assessment of security products.

<https://www.soldsecure.com/>

## Crimestoppers

An independent charity that gives people the power to speak up to stop crime 100% anonymously, by phone 0800 555 111 or online.

<https://crimestoppers-uk.org/>

## Victim Support

Covering the whole of Norfolk and Suffolk, a free, confidential support service specifically designed to help victims and witnesses of any crime.

Contact us on:

Phone: 0300 303 3706 (weekdays between 8am-5pm)

Email: [nsvictimcare@victimsupport.org.uk](mailto:nsvictimcare@victimsupport.org.uk)

Web: [www.nsvictimcare.org](http://www.nsvictimcare.org)

Socials: @nsvictimcare

---

Call us on 101. Always dial 999 in an emergency

**To see the full range of information go to:**

[suffolk.police.uk/firstprinciple](http://suffolk.police.uk/firstprinciple) or

[norfolk.police.uk/firstprinciple](http://norfolk.police.uk/firstprinciple)

Or alternatively use your mobile phone to scan this QR code.

