

LOCK UP ONLINE

YOU LOCK UP YOUR HOME, CAR AND VALUABLES BUT... DO YOU LOCK UP ONLINE?

The internet is amazing - from shopping to socialising the world is wide open to you. Think, would you give out your bank card with PIN number, leave your front door unlocked or give your computer to a stranger?

'Lock Up Online' and stop the Broadband Burglar getting into your world. Read our tips to help you avoid falling victim to Cyber Crime.



THE LOCK SMITHS

For more information and advice:
www.derby.gov.uk/lockuponline or visit:

Report fraud: www.actionfraud.org.uk
Learn more: www.getsafeonline.org.uk
Bank safer: www.banksafeonline.org.uk
Report criminal content: www.iwf.org.uk

Learn more on child online safety
www.childnet-int.org or www.ceop.police.uk

LOCK UP ONLINE

CYBERCRIME
www.derby.gov.uk/lockuponline



Join us on Facebook
[Facebook/derbycc](https://www.facebook.com/derbycc)



Follow us on Twitter
[@DerbyCC](https://twitter.com/derbycc)



Derby City Council

LOCK UP ON THE MOVE

Don't let your smartphone or tablet fall into the hands of the Broadband Burglar. Lock up on the move.



- Don't leave it on top of open bags, on seats or visible in your car
- Security Tag your phone with a UV pen and register on a site like www.immobilise.com
- Use a password or PIN to lock your device
- Record IMEI serial numbers which can be found on either the battery or SIM case. It can also be located by dialling *#06#
- Restrict alternative network usage. Non-password protected Wi-Fi connections are not only a security risk but will drain your battery
- Avoid having your bluetooth turned on, password protect it
- Make sure you know what data is saved to your phone when syncing to your computer
- Sync your phone regularly.

SCAM SAVVY

The Broadband Burglar loves a good money making scam, be one step ahead and scam savvy.

Types of scams and important tips:

Fraudulent websites

- Be aware when buying tickets and holidays online
- Stick to reputable sites
- Do research and check out reviews.

Fake e-mail scams

- If unsure about an email don't open it, don't click on any links or attachments
- Never reply to an email asking for money or personal details even if it appears to be from a friend
- Don't reply to threatening emails.

Auction sites

- Read the item details carefully
- Check past reviews and ask questions
- Leave feedback
- Learn more, auction sites can offer advice on safety
- Don't rush to bid on or buy items
- Don't bid more than you intended
- Don't guess or make assumptions.

Advertising

- Be aware of clever targeting, if you just announced you were engaged on Facebook you will suddenly see more wedding related adverts
- Don't sign up to something you don't want
- Don't fall for the promise of free items or false prizes.

Get rich quick

- Almost always makes you poorer not richer, steer clear.

LOCK UP AND BACK UP

Lock the Broadband Burglar out of your computer and out of your world. Lock up and back up.

Password tips

- Don't use the same password for everything
- If you change your password use something very different to the original one
- Don't keep your password near to or stored on your computer
- Don't click on 'remember' passwords
- Avoid using your birthday/anniversary/pet's name/football team etc
- Use upper and lower case letters, number and symbols.

Tips

- Use anti-virus software and make sure you are protected
- Always download updates
- Check your computer has a password when you turn it on
- Don't access your personal information on free and unsecure Wi-Fi
- Always secure your own Wi-Fi connection with a strong password
- Back up using CDs, hard-drives or a USB stick
- Encrypt your USB stick
- Check out firewalls. Lots are free and available to download online
- Don't keep personal information stored in documents or written on notes around your computer.

LOCK UP YOUR LIFE


The Broadband Burglar has many faces, don't get your identity taken or let unwanted "friends" into your social media world, lock up your life!

Social media

Facebook, YouTube and Twitter are part of everyday life. Be careful about what you post, it could be used to commit identity fraud against you.

- If a stranger asked you in the street for a piece of information, would you give it to them? If the answer is no, don't put it online
- Learn about privacy settings and share only what you want to
- Report privacy violations
- Tell your children about the risks of social networking, including online chat rooms, online gaming or clicking on things they shouldn't
- Be aware of hidden costs within games and mobile phone apps so you don't get stung with a big bill
- Find out more about password protection and parental controls.

Online shopping

- Is the website reputable?
- When making payments does a secure symbol, usually a padlock  appear in the bottom right on the screen or on the address bar?
- Is the deal too good to be true?
- Does the website seem unusual?
- Did the payment process seem strange?

Report it to www.actionfraud.org.uk the UK's national fraud reporting centre.

Online banking

- Look at a website carefully, if it doesn't seem right it probably isn't
- Don't write down banking passwords or leave near your computer
- Be wary of emails alleging to be from your bank, don't click on a link or give out your account details
- Sometimes your bank can help, if there's a problem act quickly.