Important cybersecurity warning for small businesses

Hi [FirstName],

The Cyber Resilience Centre for the East Midlands are alerting small businesses about recent cyber security threats that could impact them.
The UK's National Cyber Security Centre (NCSC) has issued new warnings about a Russian state-linked hacking group, who have been breaking into everyday internet routers to steal passwords and other private information. These routers are often the same type used in small offices and home workplaces, so you could be at risk.

Why this matters to small businesses

Small firms often rely on simple, off-the-shelf routers. If these devices are left with old software or default passwords, they become easy targets. Once a router is taken over:

- Every device connected to it, laptops, mobiles, tablets, can be quietly redirected to fake websites.
- Staff may enter real passwords into convincing copies of common services like Outlook.
- Hackers may gain ongoing access to emails, accounts, and other sensitive business information.

It's a silent threat: everything may appear normal while your data is being stolen in the background.

What actionable steps can be taken?

There are several key steps that directly help defend against this type of attack:

1. **Use strong passwords and two-step verification**
   If attackers do get into your router, stolen passwords are less useful when accounts also require a second step, like an app code, to log in.
2. **Keep your devices updated**
   Many of the hacked routers were vulnerable because they were running old software with known security gaps. Keeping routers up to date closes these holes.
3. **Secure your internet router** which may mean checking with your MSP or building management if someone else is maintaining the routers.
   The NCSC stresses how important it is to protect router settings, change default passwords, and turn off remote access if you don't need it. This makes it much harder for criminals to break in.
4. **Be alert to fake websites**
   Because attackers redirect your traffic, you may see login pages that look real but aren't. Training staff to be cautious helps reduce the risk of entering sensitive details in the wrong place.
5. **Keep an eye on your systems**
   Regularly checking router settings or unusual behaviour—like slow internet or login issues—can reveal problems early.

Your local Cyber Resilience Centre can connect you with funded Security Awareness Training, which provides practical guidance and information on the above. Small businesses can also join their CRC community for free, unlocking access to more funded cyber security services, monthly update newsletters, exclusive access to events and webinars, and more.

Join our community here:

Register for free

USEFUL CONTACTS

159 - for urgent help to contact your bank for fraud and scams

Find out how to report a fraud/cyber incident here

7726 - to report spam texts and vishing voice calls (spells SPAM on a phone keypad)

report@phishing.gov.uk - for reporting phishing email

Tell the police about cyber crime and fraud at reportfraud.police.uk or by calling 0300 123 2040

The Cyber Resilience Centre for the East Midlands, Derbyshire Constabulary Hq, Butterley Hall, Ripley, DE5 3RS, United Kingdom