



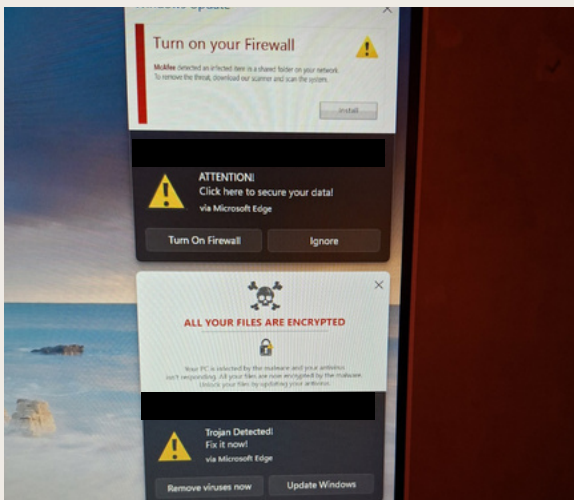
ISSUE 68

SCAMS AWARENESS NEWSLETTER

JULY 2026

WELCOME TO OUR

Monthly Newsletter



In this newsletter:

- What are scareware scams and how do they work p.2
- What you should do plus myth or fact tips p.3
- How to protect yourself and top tips to protect yourself p.4

Scareware Scams - don't panic!

Don't Panic! Understanding Scareware Scams
We've all experienced that sinking feeling when something unexpected appears on our computer screen. Imagine you're checking your emails or looking up a recipe when suddenly your screen turns bright red.

A loud alarm starts sounding.

A message flashes:

"WARNING! Your computer has been infected with 37 viruses."

Another message appears:

"Your bank details are at risk. Do not turn off your computer. Call Microsoft Support immediately on 0800 XXX XXXX."

The mouse won't seem to work properly.

The browser refuses to close.

The alarm keeps ringing.

It's enough to make anyone panic.

Fortunately, in almost every case, this isn't a genuine warning – it's a scam known as scareware.

What is scareware?

Scareware is designed to frighten you into believing that something is seriously wrong with your computer.

Criminals use fear to persuade people to act quickly without stopping to think. They want you to believe that your computer has been hacked, infected with viruses, or that your personal information is about to be stolen.

Scareware often:

- Appears as a pop-up message or fake security warning.
- Uses flashing screens, loud alarms or spoken warnings to create panic.
- Displays the logos of well-known companies such as Microsoft, Apple or antivirus companies like McAfee or Norton.
- Claims your computer has been infected with viruses or other threats.
- Urges you to telephone a support number immediately or download software to fix the problem.

As more people have become aware of phishing emails and email providers have become better at filtering them, criminals are increasingly turning to scareware because it catches people off guard and encourages them to react without thinking.

Why do these scams work?

Scammers rely on emotion rather than technology.

When we feel frightened, our natural instinct is to act quickly to solve the problem.

Unfortunately, this is exactly what the criminals are relying on.

They use:

- Flashing screens
- Loud alarms
- Countdown timers
- Urgent language
- Official-looking logos
- Warnings that your money or personal information is at immediate risk

All of these are designed to stop us thinking clearly.

The best defence is to slow down. If something tells you that you must act immediately, that's often the first warning sign that it could be a scam.



What happens if you call?

If you ring the number displayed on the screen, you'll usually speak to someone who sounds calm, friendly and professional.

They may say:

"Don't worry—we can fix this."

The scammer will often ask you to install software that allows them to remotely access your computer.

Once connected they may:

- View your personal files.
- Access saved passwords.
- Watch what you type.
- Persuade you to log into online banking.
- Install genuine malware onto your device.
- Charge hundreds of pounds for unnecessary "repairs" or fake security software.

Some scammers simply ask for payment by debit or credit card. Others remain connected for several hours while convincing victims that their computer is full of dangerous viruses.

The good news

The warning itself is rarely the real problem.

The danger begins when someone telephones the number, installs software, or gives the scammer remote access to their computer. Many scareware pop-ups are simply fake web pages designed to look frightening. Although they may seem impossible to close, they often haven't infected your computer at all.



What should you do?

If a warning suddenly appears:
Don't panic.

Take a moment before doing anything.
Never telephone the number displayed on the screen.

Do not click "Allow", "Accept" or "Download."

On a Windows computer you can:

- Disconnect your computer from the internet by turning off the Wi-Fi or unplugging the network cable.
- Press Ctrl + Alt + Delete and try closing your internet browser.
- Alternatively, restart your computer.
- If that doesn't work, ask someone you trust for help.

If the warning keeps returning, check which websites you've allowed to send notifications and remove permission for any you don't recognise. These fake alerts are often caused by browser notifications rather than a virus.

Myth or Fact?

Myth: Microsoft will telephone me if my computer has a virus.

Fact: Microsoft will never contact you unexpectedly to tell you your computer is infected or ask you to phone a support number.

Myth: A flashing warning means my computer has definitely been hacked.

Fact: Not necessarily. Many scareware messages are simply fake web pages designed to frighten you.

Myth: If I'm unsure, I should switch my computer off and ask for help.

Fact: Absolutely. Taking your time and asking someone you trust is one of the best ways to stay safe.



Remember...

REMEMBER

Real technology companies do not display emergency pop-ups asking you to telephone them. Microsoft, Apple and genuine antivirus companies will not suddenly lock your computer and demand that you call a support number.

Your bank certainly won't ask you to ring a telephone number displayed in a pop-up warning.

Protect yourself



A few simple habits can make a big difference:

- Keep your computer updated.
- Use reputable antivirus software.
- Never allow remote access unless you contacted the company yourself.
- Be cautious when clicking adverts or unfamiliar links online.
- If you're unsure, stop and ask someone you trust before taking any action.

Need a bit of extra digital support?



You don't have to face technology on your own. If using a computer, tablet or smartphone sometimes feels confusing or overwhelming, there are organisations that can help you build your confidence in a safe and supportive environment.

Many local libraries offer free digital support sessions, helping people learn everyday skills such as using the internet safely, spotting online scams and getting the most from their devices. Some libraries also run IT Buddy or Digital Buddy schemes, where volunteers provide one-to-one support.

The charity AbilityNet also offers free digital support for older people and disabled adults. Their volunteers can help with everything from using email and video calls to staying safe online and making devices easier to use. Learning a few simple digital skills can make it much easier to recognise scams and know what to do if something unexpected appears on your screen. Remember, asking for help isn't a sign that you're "no good with technology" - it's one of the best ways to stay safe online. Even experienced computer users are caught out by scams from time to time.

Where to get help



If you're worried about a suspicious message or think you may have been targeted:

- Speak to a trusted friend or family member.
- If you've made a payment or shared financial information, contact your bank immediately by calling 159.
- Forward suspicious emails to report@phishing.gov.uk.
- Report fraud to Report Fraud on 0300 123 2040 or online at [Report Fraud](https://www.report-fraud.org.uk)

Where to get help

Scammers want you to panic.

The safest thing you can do is exactly the opposite.

- ✓ Pause.
- ✓ Don't click.
- ✓ Don't phone the number.
- ✓ Ask someone you trust.

A genuine company will never mind if you take a little time to check.

Stopping for just a few minutes could prevent months of worry.



If you are affected by the content of this bulletin, you can talk to us. Our Scams Awareness and Aftercare Team can offer free support, advice and guidance. Contact our team today on:



01625 612958 (OPTION 5)



scams@ageukcheshire.org.uk