BITWISE-IT BUSINESS TOOLKIT

Ransomware

How it happens, what to do in the first hour, and how to make it unlikely

Bitwise-IT Limited

Wickford, Essex · 01268 218301

info@bitwise-it.co.uk · bitwise-it.co.uk

What you are dealing with

> Ransomware encrypts your files and demands payment for the key. Modern attacks usually steal a copy of the data first, so that refusing to pay carries a second threat: publication. Small businesses are targeted precisely because they are less defended, not because they are less valuable.

The uncomfortable part is that the encryption is the *end* of the attack, not the beginning. By the time you see the ransom note, an attacker has typically been inside for days or weeks — reading email, mapping the network, and finding your backups.

How it gets in

Route	What it looks like
Stolen credentials	Somebody signs in with a real password bought from an old breach. No malware, no alarm, no clever trick. The most common route by far.
Phishing	An attachment or link that looks routine — an invoice, a delivery note, a shared document.
Unpatched systems	A known flaw in something exposed to the internet, fixed by the vendor months ago and never applied.
Remote access	Remote desktop or a VPN appliance left open, with a weak password and no multi-factor authentication.
A supplier	Access granted to a third party, then abused after they are compromised.

Warning signs before the ransom note

- Sign-in alerts from places nobody has been
- Mailbox rules nobody created — particularly ones that move messages to a folder nobody reads
- Security software disabled or removed on a machine, with no explanation
- New user accounts, or existing accounts suddenly given administrator rights
- Your backup tool proposing to delete a very large number of files you did not delete
- Machines busy overnight, or unusually slow for no apparent reason

> **THAT LAST ONE DESERVES EMPHASIS**
> If a backup or sync job suddenly wants to change or delete thousands of files, stop it. That is what mass encryption looks like from a backup tool's point of view — and if you let it run, it faithfully replaces your good backup with the encrypted version.

The first hour

> What you do in the first hour has more effect on the outcome than anything that follows. Print this page and keep it somewhere you can reach without a computer.

1. **Disconnect, do not switch off**

   Unplug the network cable and turn off Wi-Fi on affected machines to stop it spreading. **Leave them powered on.** Shutting down destroys evidence held in memory that can sometimes help with recovery, and occasionally holds the encryption key.

2. **Do not connect your backups**

   Not the external drive, not the NAS, nothing. Connecting a clean backup to an infected network is the most common way businesses lose their last good copy. Leave them disconnected until someone competent says otherwise.

3. **Get help**

   Call your IT support. If you do not have any, call us on **01268 218301** — we would rather talk you through the first steps than watch a business make the situation worse for free.

4. **Report it**

   Call **0300 123 2040**. Action Fraud, now branded Report Fraud, staffs this line around the clock specifically for organisations under live attack, and it is the national reporting route for England, Wales and Northern Ireland.

5. **Change passwords from a clean device**

   Starting with email and any administrator accounts — but do it from a phone or a machine you know is unaffected, never from the compromised one.

6. **Tell your insurer, early**

   Cyber policies frequently require prompt notification and often insist on their own incident responders. Calling in your own people first can void the cover.

7. **Consider the 72-hour clock**

   If personal data may have been accessed, UK GDPR may require you to notify the ICO within 72 hours of becoming aware. Take advice quickly — the clock does not wait for the investigation to finish.

8. **Write down what happened, as it happens**

   Times, screens, what was clicked, who was told. Insurers, the ICO and the investigators will all want it, and nobody remembers accurately a week later.

> **SHOULD YOU PAY?**
>
> Law enforcement advises against it, and there are practical reasons beyond principle. Payment does not guarantee a working key, decryption tools are frequently slow and incomplete, it does nothing about data that has already been copied out, and it marks you as an organisation that pays. There may also be legal complications depending on who is being paid. Take proper advice before anyone even considers it — and note that having a tested backup is what removes the question entirely.

Making it much less likely

> No single control stops ransomware. Layers do — and the useful ones are neither exotic nor expensive.

Layer	Why it matters
Multi-factor authentication	Removes the most common way in outright. Free with Microsoft 365. If you do one thing, do this.
Patching, provably	Most successful intrusions use a flaw fixed months earlier. "Updates are on" is not the same as "updates are working" — somebody should be checking.
An offline or immutable backup	A backup the attacker cannot reach or alter is what turns this from an extinction event into a bad week.
Least privilege	Nobody works day to day as an administrator. It limits how far an intrusion can spread from any one machine.
Email filtering	Stops most of it arriving at all. Worth more than the standard default.
Trained people	Someone who reports a strange email at nine o'clock saves the day that would otherwise start at midnight.
Monitoring	The attack takes days or weeks. Somebody watching for the signs is what turns a catastrophe into an incident.

Backups that survive an attack

Ransomware operators look for backups deliberately, and encrypt them first where they can. A backup only helps if the attacker cannot reach it, so:

- [ ] Keep at least one copy **offline** — disconnected between runs, not permanently plugged in
- [ ] Or use backup storage that is **immutable**, meaning it cannot be altered or deleted for a set period even with valid credentials
- [ ] Make sure your **Microsoft 365 data** is included; encrypted files sync to the cloud like any other change
- [ ] **Test a restore** regularly. An untested backup is a hope, not a plan
- [ ] Protect the backup system with its own credentials and its own multi-factor authentication

> **THE HONEST SUMMARY**
>
> Businesses that recover well are almost never the ones with the cleverest security. They are the ones who had multi-factor authentication on, patched reliably, kept a backup out of reach, and knew who to call. All four are within reach of a five-person company.

Prevention is considerably cheaper

We build the layers above into how we look after clients as standard: managed backup including Microsoft 365, monitoring and patching, layered email protection, and security awareness training so your team spots the message that starts it all.

If you would like to know how exposed you currently are, we will take a look and tell you honestly.

01268 218301 · info@bitwise-it.co.uk · bitwise-it.co.uk