Cyber security review

Larch & Lathe Joinery · Kirkcaldy · 9 staff

November 2026 | Prepared by Universal Computing

EXAMPLE Larch & Lathe Joinery is a made-up business. Every finding in this example is made up too, to show the format of our report.

OVERALL	CHECKS PASSED	TO FIX SOON	CYBER ESSENTIALS
Amber	28 of 40	9	3 of 5
3 to fix first	28 in good shape	amber findings	controls ready

In short

- Two accounts, including the owner's, can be signed into with just a password, and one mailbox copies every email to a personal Gmail address.
- Backups run every night, but nobody has tried a restore, and email, OneDrive and SharePoint aren't backed up.
- Devices are well looked after apart from one Windows 10 laptop and the router's software. Fix those and the account issues, and Cyber Essentials is within reach.

Fix these first

RED · EMAIL AND MICROSOFT 365

Two accounts without multi-factor sign-in

Switch it on for both, starting with the owner's account. It's quick, and we can do it with you on a call.

RED · EMAIL AND MICROSOFT 365

Every email in one mailbox is copied to a personal Gmail address

Remove the rule. Work email can be read at home in Outlook once multi-factor sign-in is on for every account.

RED · ACCOUNTS AND ACCESS

A former employee's account is still active

Block sign-in today. Keep the mailbox if you need it, and check every account against your staff list.

How to read this report

STATUS

Red	**Fix now**	An attacker could use this today.
Amber	**Fix soon**	It weakens your protection, or it would stop you passing Cyber Essentials.
Green	**Good**	Keep it that way.

EFFORT

Quick	under an hour
Medium	a few hours
Larger	a day or more, or something to buy

Who: You, Us, or You or us.

01 · Email and Microsoft 365

Multi-factor sign-in on every account, admin accounts, old sign-in methods, forwarding rules that send mail outside the business, and your email filtering.

CHECK	STATUS	WHAT WE FOUND	WHAT TO DO
Multi-factor sign-in on every account	Red	Seven of the nine staff accounts ask for a code. The owner's account and the office manager's account don't.	Switch on multi-factor sign-in for both, starting with the owner's account. Who: You or us · Effort: Quick
Admin accounts	Amber	Two people have full admin rights, and both use those accounts for everyday email.	Give each of them a separate admin account, used only for admin work. Who: Us · Effort: Quick
Old sign-in methods	Green	Switched off for every account, so a password alone can't be used through older email apps.	
Forwarding rules	Red	One person's mailbox copies every email to their personal Gmail address, to read it at home.	Remove the rule. They can read work email at home in Outlook once multi-factor sign-in is on for every account. Who: Us · Effort: Quick
Spam and malware filtering	Green	Filtering is on, and suspicious emails are held in quarantine.	
Alerts for unusual sign-ins	Green	Alerts for risky sign-ins and new forwarding rules go to the owner.	
Protection against spoofed email (SPF, DKIM and DMARC)	Amber	SPF is set up. DKIM isn't switched on, and DMARC only monitors.	Switch on DKIM, then set DMARC to quarantine once its reports look clean. Who: Us · Effort: Quick
Apps with access to mailboxes	Green	Only your accounts software has access, and it's still in use.	

8 checks: 2 red, 2 amber, 4 green

02 · Accounts and access

Former staff, shared logins, who has admin rights, how passwords are managed and who can see your shared files.

CHECK	STATUS	WHAT WE FOUND	WHAT TO DO
Former staff	Red	An account for someone who left in March is still active.	Block sign-in today. Keep the mailbox if you need it, and check every account against your staff list. Who: You or us · Effort: Quick
Everyone has their own login	Green	No shared logins on computers or in Microsoft 365.	
Passwords	Amber	There's no password manager, and some staff use the same password for several things.	Use a business password manager, so every account can have its own strong password. Who: You or us · Effort: Medium
Admin rights on computers	Green	Staff don't have admin rights on their laptops.	
Shared files	Green	SharePoint and OneDrive files are shared with named people, and nothing is shared with anyone who has the link.	
Guest accounts	Green	Two guest accounts, both for your accountant, and both still needed.	

6 checks: 1 red, 1 amber, 4 green

03 · Computers, laptops and phones

Security updates, older systems that no longer get them, antivirus, disk encryption, screen locks and the phones that get your email.

CHECK	STATUS	WHAT WE FOUND	WHAT TO DO
Security updates	Green	Every supported computer installed its updates in the last month.	
Unsupported systems	Amber	One laptop still runs Windows 10, whose support ended in October 2025.	Upgrade it to Windows 11 if the laptop can run it, or replace it. Who: You · Effort: Larger
Antivirus	Green	Microsoft Defender is on and up to date on every computer.	
Disk encryption	Green	BitLocker is on for every laptop, so nobody can read the data on a lost or stolen laptop.	
Screen locks	Green	Screens lock after five minutes.	
Phones with work email	Green	Every phone that gets work email has a screen lock and is up to date.	
Software on computers	Green	No unsupported or unwanted apps found.	

7 checks: 0 red, 1 amber, 6 green

04 · Backups and recovery

What's backed up, Microsoft 365 included, whether a copy is kept away from your network, and whether a restore has ever been tested.

CHECK	STATUS	WHAT WE FOUND	WHAT TO DO
Office files	Green	Files on the office NAS are backed up to the cloud every night.	
Email, OneDrive and SharePoint	Amber	They aren't backed up. Microsoft keeps deleted items for a limited time only.	Add a Microsoft 365 backup. Who: Us · Effort: Medium
A copy away from your network	Green	The cloud copy can't be changed or deleted from the office network.	
Restores tested	Amber	Nobody has tried restoring a file.	Test a restore this month, then every three months. Who: Us · Effort: Quick
Backup alerts	Green	A failed backup sends an email to the office manager.	

5 checks: 0 red, 2 amber, 3 green

05 · Wi-Fi, router and remote working

Router passwords and updates, guest Wi-Fi, open connections from the internet, how staff connect from home, and your website from the outside.

CHECK	STATUS	WHAT WE FOUND	WHAT TO DO
Router admin password	Green	Changed from the one printed on the router.	
Router updates	Amber	The router's software is two versions behind.	Update it out of hours. Who: Us · Effort: Quick
Remote access and open connections	Green	Staff working from home use Microsoft 365, nothing unexpected is open, and remote desktop isn't reachable from the internet.	
Guest Wi-Fi	Green	Visitors use a separate guest network that can't see office devices.	
Wi-Fi security	Green	WPA2 with a long password.	
Your website from the outside	Green	Its security certificate is valid, and its software is up to date.	

6 checks: 0 red, 1 amber, 5 green

06 · People, payments and phishing

How staff spot phishing, how bank detail changes are checked, what happens after a wrong click, and whether you have a plan and cyber insurance.

CHECK	STATUS	WHAT WE FOUND	WHAT TO DO
Reporting suspicious emails	Green	Staff know how to report a suspicious email, and they do.	
Changes to bank details	Amber	Bank detail changes are usually checked by phone, but the rule isn't written down.	Write down the rule. Before changing bank details, always phone the supplier on a number you already have. Who: You · Effort: Quick
Approving payments	Green	Two people approve any payment over £1,000.	
After a wrong click	Green	Staff know to call the office manager straight away.	
A plan for the worst day	Amber	There's no written plan for a cyber attack.	Pin up the one-page plan at the end of this report. Who: You · Effort: Quick
Cyber insurance	Green	Cover is in place, and the policy has a helpline for incidents.	
Staff training	Green	Staff had phishing awareness training this year.	
Staff emails in known data breaches	Green	Four staff addresses appear in breaches of other websites. All four have since changed those passwords.	

8 checks: 0 red, 2 amber, 6 green

Cyber Essentials readiness

CONTROL	STATUS	WHAT WE FOUND
Firewalls	Ready	The router's firewall is on, nothing unexpected is open, and the firewall is on for every laptop.
Secure configuration	Ready	Default passwords changed, screen locks set and unused software removed.
Security update management	Not yet	One laptop runs Windows 10, whose support ended in October 2025, and the router's software is out of date.
User access control	Not yet	Two accounts without multi-factor sign-in, a former employee's account and admin accounts used for everyday email.
Malware protection	Ready	Microsoft Defender on every computer.

Fix the two controls marked Not yet and you're ready to apply, with 75% off a new certificate through the Cyber Essentials First Step Fund until the end of March 2027, or until the funding runs out.

Your plan

WHEN	WHO	WHAT
This week	You	Approve multi-factor sign-in for every account, and we'll switch it on with your team.
	Us	Remove the forwarding rule and check that mailbox's recent sign-ins.
	You	Block the former employee's account, or ask us to.
This month	You	Write down the rule that bank detail changes are checked by phone, and pin up the one-page plan at the end of this report.
	Us	Set up separate admin accounts and switch on DKIM.
	Us	Test a restore and add a Microsoft 365 backup.
Next three months	You	Upgrade or replace the Windows 10 laptop, and start using a password manager.
	Us	Update the router and set DMARC to quarantine.
Then	You	Apply for Cyber Essentials, with 75% off through the First Step Fund until the end of March 2027, or until the funding runs out.

Free resources

NCSC Cyber Action Toolkit Free, personalised steps for sole traders and small businesses.	https://cybertoolkit.service.ncsc.gov.uk/
NCSC advice for small businesses NCSC guidance for small and medium-sized organisations.	https://www.ncsc.gov.uk/section/advice-guidance/small-medium-sized-organisations
Cyber Essentials First Step Fund 75% off a new Cyber Essentials certificate, through IASME.	https://firststep.iasme.co.uk/

About this report

- **What we looked at:** your answers to our form, your settings in an online session with you, and your business from the internet, with your permission.
- **What it isn't:** a penetration test or a Cyber Essentials assessment.
- We never asked for, or saw, your passwords.
- **When to check again:** in a year, or after a big change such as new staff, a new office or a new system.

Questions about your report? Call 01383 840808 or email info@universalcomputing.co.uk.

If something goes wrong

UNIVERSAL COMPUTING
01383 840808

1. **Call us**
   Ring **01383 840808**, Monday to Friday, 9am to 5pm. If you're a client out of hours, raise an urgent support ticket.

2. **Disconnect from the network**
   Unplug the network cable or turn off Wi-Fi on any computer you think is affected.

3. **Change passwords**
   From a computer or phone you trust, change the password of any account you think is affected.

4. **Money or bank details**
   Call your bank straight away.

5. **Report it**
   Report the crime to Police Scotland on **101**.

6. **Personal data**
   If customer or staff details may have been taken, check straight away whether you must report it to the ICO. The deadline is 72 hours from finding out.

7. **Insurance**
   Call your cyber insurer's helpline if you have cover.

8. **Keep notes**
   Write down what happened and when. It helps us, your bank, the police and your insurer.

Forward suspicious emails to **report@phishing.gov.uk** and scam texts to **7726**.