1. Lock the doors

List every account, use a password manager, turn on two-step sign-in, remove access the same day.

LoftyBiz
loftybiz.net

1 Five moves

Move	What to do	Example (Milica, Podgorica)
1 List every account	Email, bank, accounting, cloud storage, website, domain, social pages. Who can get in? Move 4 still tied to an assistant who	Found 23 accounts, 4 still tied to an assistant who
2 A password manager	A long, unique password for every account. Each person gets their own login. Share person accounts so more shares, not pas	About $4 a person a month. Not more shares, not pas
3 Two-step sign-in	Start with email, bank, payments and accounting. Prefer an authenticator app over text message.	A stolen password alone is not enough.
4 Remove access the same day	Change shared passwords that person used, remove their accounts, check connected systems. Review the whole list on 30 mi	Accounts in Systex. Review the whole list on 30 mi
5 Look after devices	Automatic updates on, a screen lock on every laptop and phone, the disk encrypted, remote wipe switched on	A lost laptop is an inconvenience, not a crisis.

2 Illustrative result

Milica, bookkeeping office in Podgorica, 4 staff, about 60 small-business clients. After a break-in that used a shared password: within 6 months, two-step sign-in covered all 23 accounts (up from 3); former staff with access went from 2 to 0; removing access now takes about 15 minutes. Two new clients chose her office partly because she could explain how their data is protected. These are examples, not promises. Example figures. General education, not financial advice. Results vary. This is general education, not security advice. Follow your providers' guidance and ask an IT professional.

2. Plan for the bad day

Three-two-one backups, a monthly restore test, a call-back rule, team training, a one-page plan.

LoftyBiz
loftybiz.net

1 Five steps

Step	What to do	Example (Hafiz, Kuching)
1 Three-two-one backups	Three copies of what matters, on two kinds of storage, with one copy so [illegible]	Laptop and shared files backed up automatically ev
2 Test a restore monthly	Pick one folder and bring it back from the backup. Time it. A backup you [illegible]	First test failed the backup had stopped 6 weeks e
3 A payment-change rule	Confirm any request to change bank details by calling a number you already [illegible]	The step that stops most invoice scams. The email. Ne
4 Teach the warning signs	Hurry. Secrecy. A new way to pay. A link asking you to log in. A sender [illegible]	Ten minutes later off. Thank a team, who reports al
5 A one-page bad-day plan	Who to call first, which passwords to change, where the backups are, what to tell customers. Keep a printed copy [illegible]	Bank, platforms and KIT helpline on the first-call lis

2 Illustrative result

Hafiz, online shop in Kuching, 3 staff, average order about $45, about 300 orders a month. After a failed drive that took 3 days to rebuild, and a near-miss $1,200 fake invoice: a stolen staff laptop was replaced and the team was working again in about 3 hours, with no orders lost. The payment rule blocked two fake invoices worth about $2,000 together. These are examples, not promises. Example figures. General education, not financial advice. Results vary. This is general education, not security advice. Follow your providers' guidance and ask an IT professional.

3. This week

A short lock-up list, and a monthly reminder.

1 Do this week

List every account and who can get in	[ ] Done
Turn on two-step sign-in for email, bank and payments	[ ] Done
Set up a password manager for the team	[ ] Done
Switch on an automatic backup and test one restore	[ ] Done
Set a monthly reminder in Systex (our own product, loftybiz.net) to test a restore	[ ] Done
Write your payment-change rule and put it on every desk	[ ] Done

2 Watch-outs

Doors: reusing one password; sharing logins in chat or email; making the owner the only person who can get in. Bad day: a backup that lives next to the original; trusting a familiar name or voice (emails, caller ID and even voices can be faked with AI); slow, blame-heavy reporting.

Milica, Hafiz and their figures are illustrative. These are examples, not promises. Example figures. General education, not financial advice. Results vary. This is general education, not security advice. Follow your providers' guidance and ask an IT professional. Free tool from LoftyBiz. Systex (our own product): loftybiz.net