Your ex-receptionist might still have access to your email.

That's a SECURITY RISK waiting to happen.

Kriston Technology

When someone leaves your business do **ALL** their logins leave with them?

Email.

Files.

Apps.

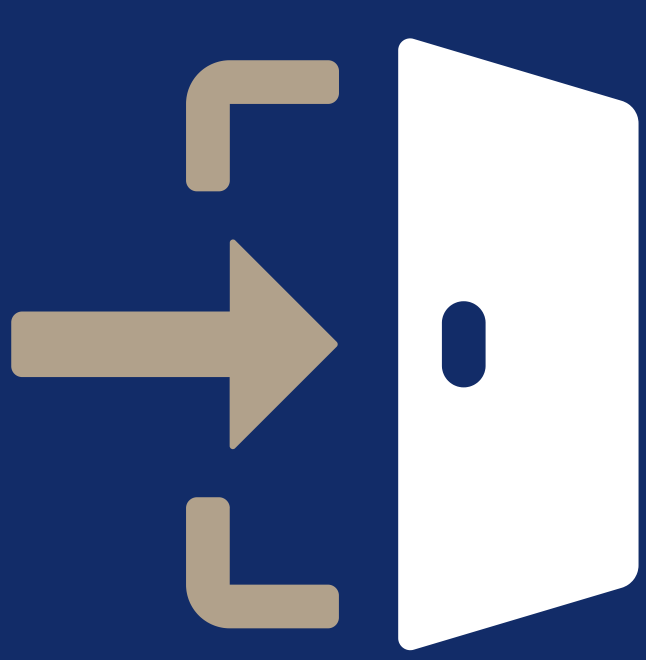
Remote access.

It’s easy to miss one.

Kriston Technology

Ex-staff accounts are one of the easiest ways into a business.

No hacking necessary.



Kriston Technology

Those accounts often still have:

- **Access to sensitive data**
- **Permissions to change things**
- **No one actively monitoring them**

Perfect for **misuse.**

Kriston Technology

It’s not always malicious.

Sometimes it’s:

- A saved password on an old device
- An account forgotten in a system
- Access that was temporary... but never removed

Kriston Technology

Could a former employee **still...**

- **Read your emails?**
- **Access client data?**
- **Log into your systems from home?**

If you're not **100% sure,** that's a problem.

Kriston Technology

Accounts slip through because access is spread everywhere:

Microsoft 365.

Cloud apps.

Finance tools.

CRM systems.

Kriston Technology

Here's how to **spot** forgotten accounts:

- **Review your user list regularly**
- **Look for accounts that haven't been used recently**
- **Check for duplicate or generic logins ("info@" or shared accounts)**

Kriston Technology

Are there accounts that:

- No one “owns”?
- Were set up for old staff or suppliers?
- Still have active licenses?

Kriston Technology

To shut them down properly:

- Disable access immediately when someone leaves
- Transfer ownership of files and emails
- Remove licenses and permissions

Don’t leave it for later.

Kriston Technology

Build a simple offboarding process.

When someone leaves, you follow the same checklist every time.

Kriston Technology

Former employees shouldn't have a key to your business, even by accident.

We can help you find and disable unused accounts.

Get in touch.

Kriston Technology