CICADA | RESOURCES

LESSON 01 OF 04 · 7 MIN · WORKING KNOWLEDGE

Email is the master key

Why the mailbox is the highest-value account you own, and what to check if you suspect it's been accessed.

The reset button for everything

Banking, accounting, payroll, social media, your domain, your website: almost every account can be reset through your email. An attacker who can read your inbox often doesn't need to break anything else.

That's why email gets MFA first, a strong unique password, and the strictest joining and leaving process.

Secure it like a bank account

- MFA enforced for every mailbox, including shared and role addresses.
- A password manager, not a reused password.
- Automatic forwarding to external addresses blocked or reviewed.
- Inbox rules monitored for hidden rules that hide replies.
- Active sessions and connected apps reviewed.
- SPF, DKIM and DMARC published for your domain.

Signs someone has been in

Look for rules that move or delete certain messages, forwarding to an unknown address, sent items you didn't send, password-reset emails you didn't request, or sign-ins from unexpected locations. Check the audit log, not just the inbox.

If you suspect access: change the password from a different device, revoke sessions, remove unknown rules and forwarding, check MFA methods, and tell your contacts to be wary of messages from your address.

SHARED MAILBOXES

Info@ and accounts@ are still accounts. Give named people access through delegation rather than sharing a password, enforce MFA, and remove access when roles change.

Key takeaways

- ✓ Email is the reset route for almost every other account.
- ✓ Enforce MFA and block external forwarding.
- ✓ Review inbox rules, sessions and connected apps for signs of access.
- ✓ Shared mailboxes need named access and MFA too.

Generated free at resources.cicadacs.com · General guidance, not an audit or legal advice.