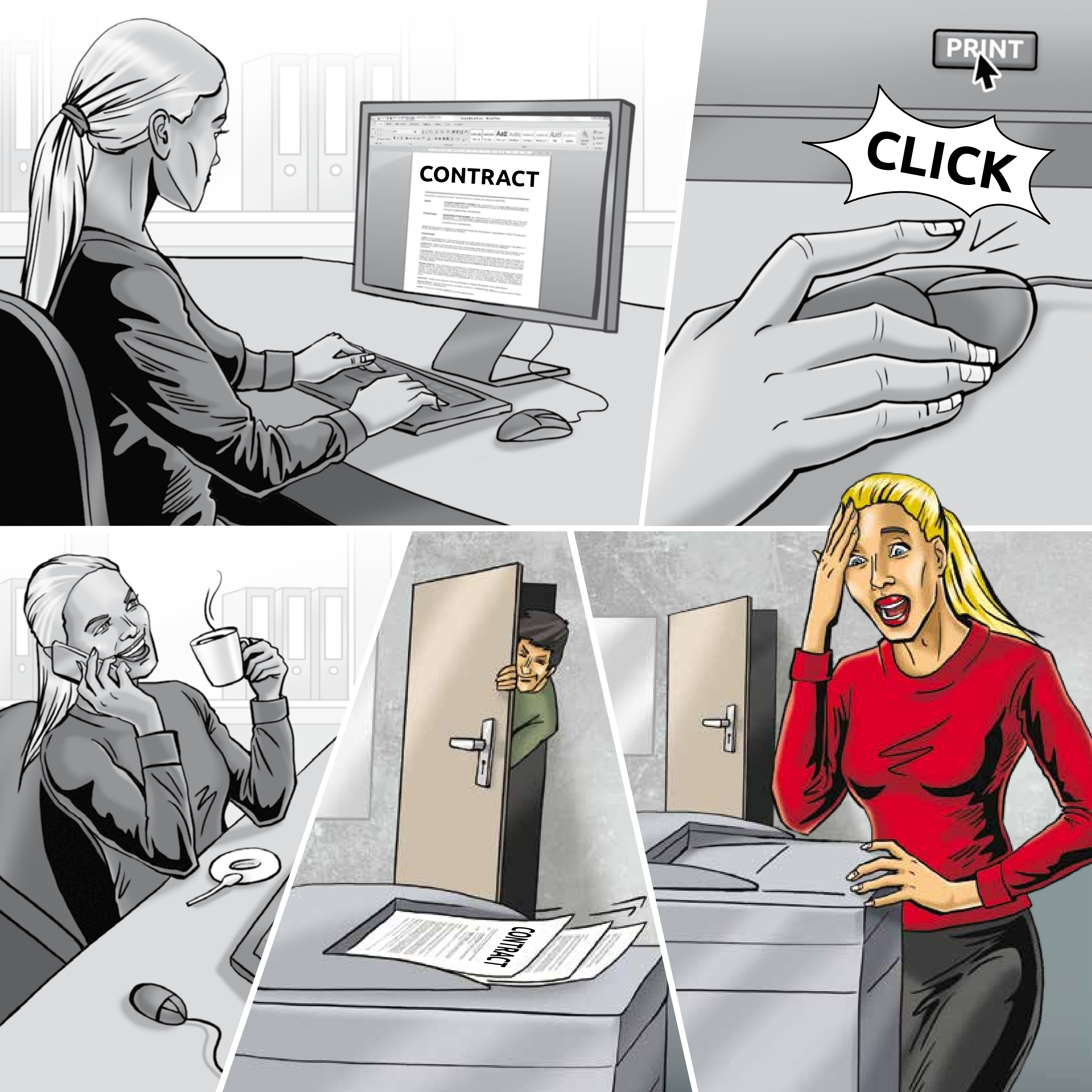
SECURE
YOUR PRINT
ENVIRONMENT
myQ
Jan Novak


CONTRACT
PRINT
CLICK
CONTRACT

CAN YOU IMAGINE...

1. Securing your data on any device you use

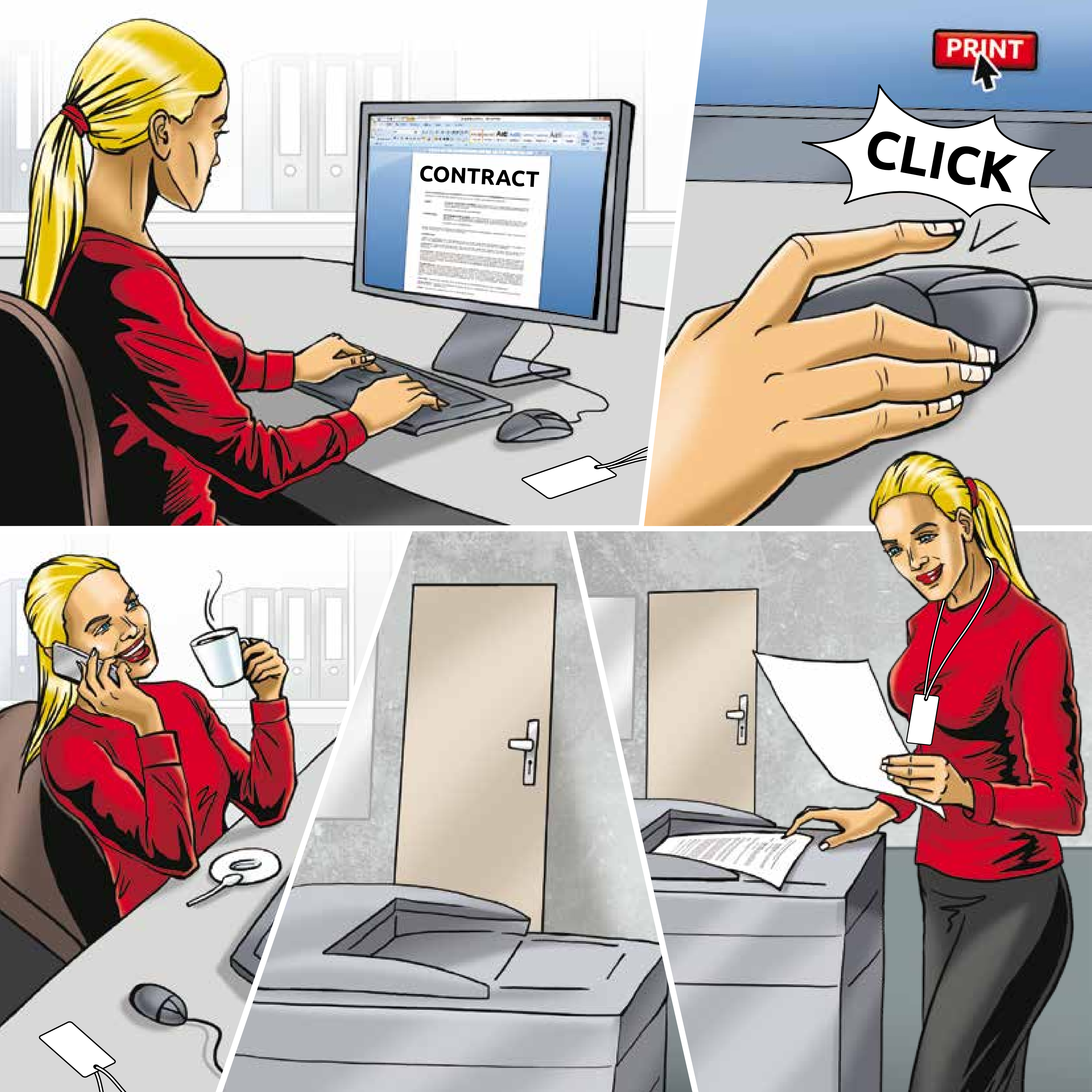
Printing, scanning and copying can be a high-security risk, even though most people don’t realize it. The lack of awareness and focus about possible security exposures make this area more vulnerable to insider threats.

2. Having to print-and-run

Imagine printing some confidential documents only to find that when you got to the printer, they weren’t there. This method of “direct print” leaves your documents unclaimed, increasing the chance of fraud, and is the least secure method of printing in a multi-device office environment.

3. Having to print-and-seek

What if you accidentally chose the wrong printer? You’d end up either running around, checking all the printers, or you would reprint the document a second time, without getting the first copy. When your organization has multiple devices, it’s crucial to know which device will print your documents.


CONTRACT
PRINT
CLICK

MYQ PROVIDES COMPLETE, CONTINUOUS SECURITY TO PROTECT YOUR PRIVACY

Your MFD is **crucial**

Print management enables organizations to benefit from their multifunctional device's technological capabilities, increased productivity, and workflow security—all in a cost-effective way.

Every device is yours

MyQ allows you to print your job from any device on the network. This also takes the guess work out of, "which printer did I choose," because with MyQ, every device is yours.

Get the security **balance** right

The user, administrator, and company each have their own security expectations, which is why MyQ provides the ability to control every aspect of the print environment.

Ideal state

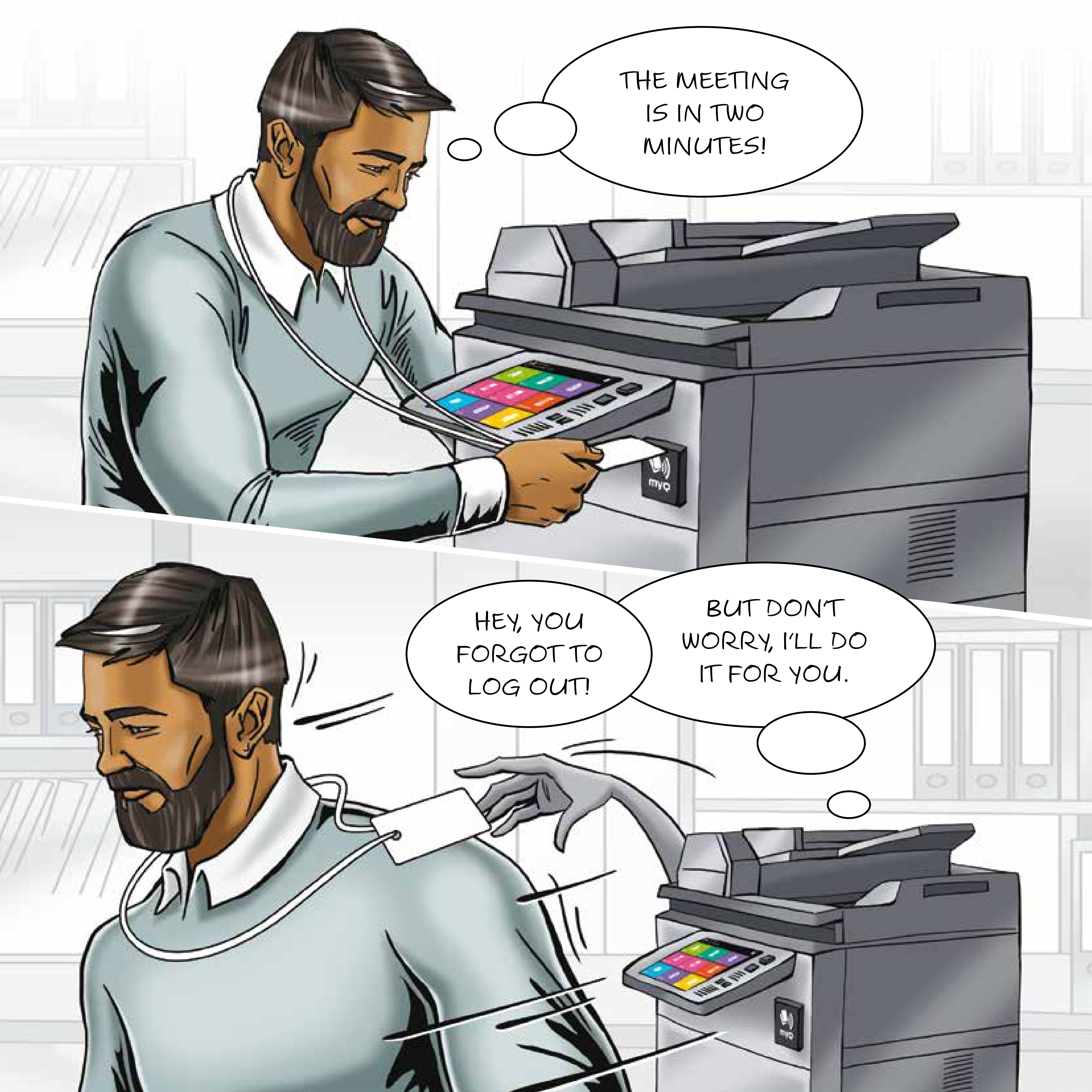
Pull printing holds jobs in the server or on the client's computer until the user authenticates themselves at the device and prints their jobs; controlling the flow of documents and allowing for optimum security.

With MyQ, the **choice** is yours

MyQ fulfills the security needs of organizations by incorporating best-in-class tools which give them the flexibility to create their own settings.

Security **policies** and **trends**

Technology is constantly evolving to make our lives easier at home and the office, which is why we emphasize adapting our security policies to keep up with current trends and legislations.


THE MEETING IS IN TWO MINUTES!
HEY, YOU FORGOT TO LOG OUT!
BUT DON'T WORRY, I'LL DO IT FOR YOU.

SECURE USER PRIVACY

GDPR Compliant

Users receive all their data, admin can anonymize accounts, and have messages about their rights on their MyQ Web Interface.

Pull Printing

Users can release jobs from any device on the network after they have authenticated themselves via PIN, ID badge, username and password, or QR code. Or combination of all „two factor autethication“.

MyQ Device Login/Logout

When MyQ Authentication is activated, the device's memory is automatically cleared after the user logs out.

Document Security

Print files are stored at the MyQ Server in a predefined folder and the admin can set a period after which the files are automatically deleted.

Private Queues

The MyQ admin can enable private queues for users or departments, where print jobs are deleted immediately after they are released.

Privacy Mode

Only owner of the job can see its name, it´s also applicable for web UI and reports.

PREVENT UNAUTHORIZED ACCESS

Complete Coverage

Once MyQ has been implemented, administrators can secure the print server, company data, and network communication.

Strengthened Policies

MyQ enforces an organization's own security policies by providing extensive security options for the MyQ Server.

Monitor Misuse

MyQ tracks all changes on the admin level and saves them to the MyQ Audit Log to detect misuse of the extended rights.

SECURED ACCESS TO THE MYQ SERVER

Interface Access

Access to the MyQ Web Interface for common users should be limited only to their profile.

Limited Access

Extend users' access rights according to their role and responsibilities in the MyQ system.

Full Access

The only accounts that have full access to the administration of MyQ are accounts with the system administrator role.

GREAT!
THE WHOLE NETWORK
IS SECURED!
myQ

CONTROLLING THE PRINT ENVIRONMENT

Watermarking

Overlay a watermark to identify the document as confidential, add the print date, and include the name of the person who printed it and from which machine it was printed. Watermark can be in format of plain text, QR or BAR code.

Job view

Admins, manager and even users can preview print jobs that have been sent to MyQ in PCL 5, PCL 6, and Postscript with third-party software.

Job Archiving

Admins and managers can keep track of what's been printed, scanned and even copied. This data can be used as a source for detailed auditing — deleting jobs in the server has no effect on files stored within this feature.

Control scanned documents

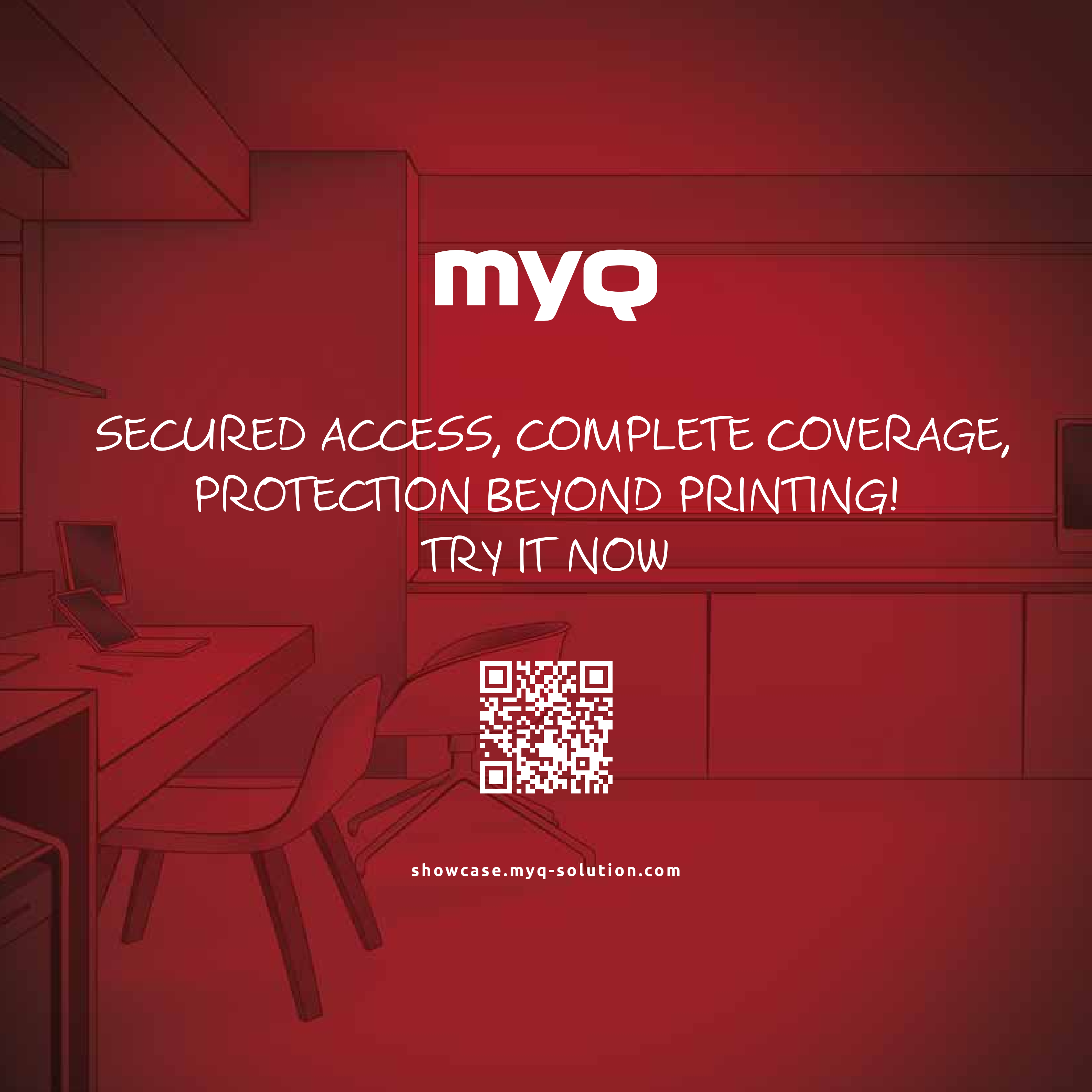
Restrict scanning to predefined folders and use an integrated OCR or DMS system. Scan workflow can be set by admins, users are allowed to scan only to folders or other destination based on the internal policy.

Track all jobs

System administrators can directly monitor and enforce company workflow security policies in your entire printer fleet.

Encryption of all data

All data, whether it´s user - server - printer communication (IPPS) or reading the status data from printers are encrypted (SNMP.v3). In addition, MyQ can encrypt the entire database.



myQ

SECURED ACCESS, COMPLETE COVERAGE,
PROTECTION BEYOND PRINTING!

TRY IT NOW

showcase.myq-solution.com