

STOKOE

COMMUNICATIONS

Worried About Your Poor Cell Reception?

You should get new signal boosters.
Contact us for a free on-site evaluation
and get your signal upgraded today.



This edition our product feature is Wilson Cell Boosters. We have supplied/installed over 1000 systems from single basic units to multi unit industrial applications. It's so important to have clear cell phone reception and the improvement is remarkable. We offer a free site evaluation so if you need a solution we are here to help.

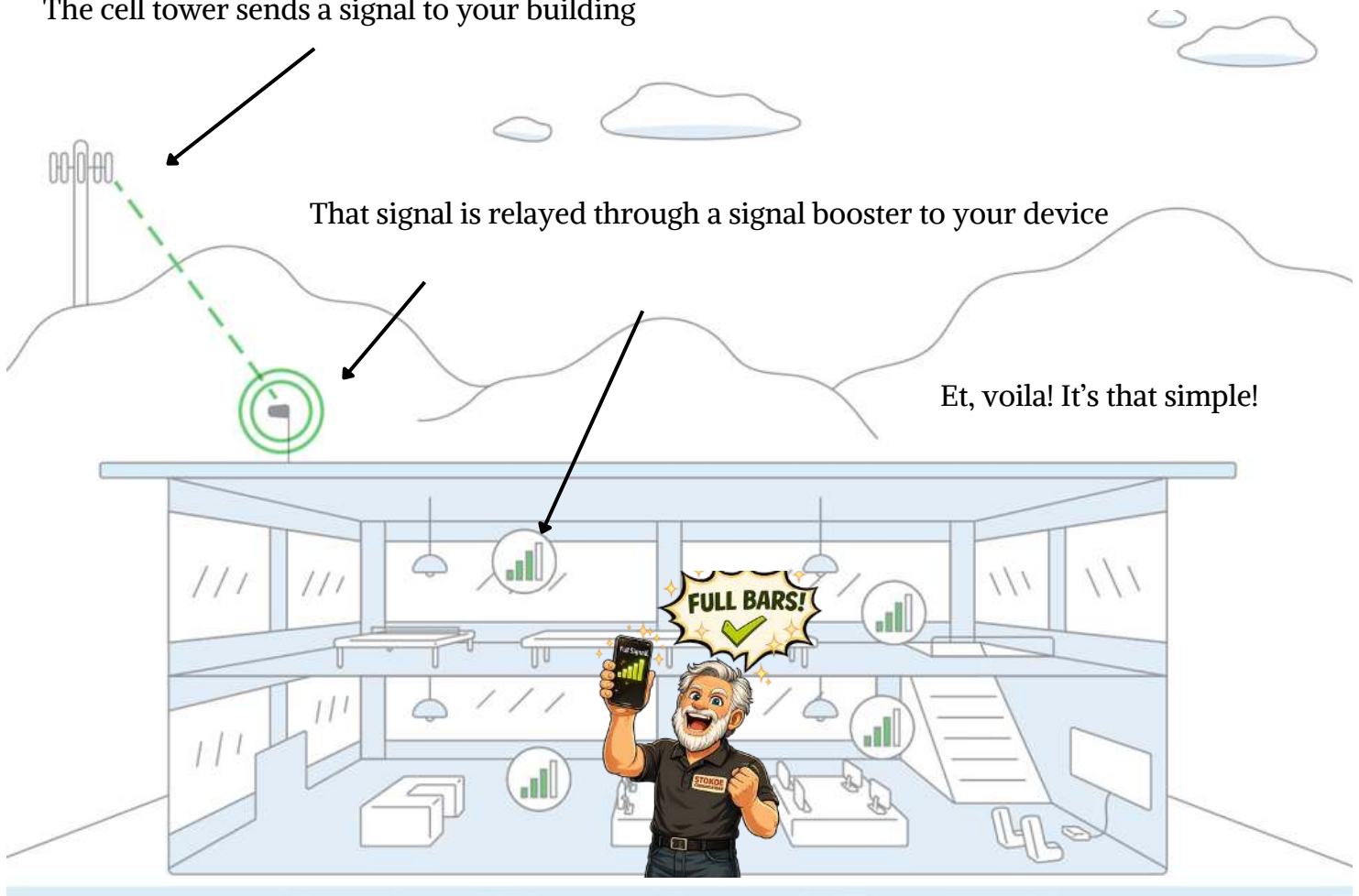
– Dave

How it works:

The cell tower sends a signal to your building

That signal is relayed through a signal booster to your device

Et, voila! It's that simple!



REQUEST FREE EVALUATION

www.stokom.com

A Recent Security Incident

We regret to say that even we are not immune to hacks and scams. On Monday, May 4th, one of our email accounts was compromised via a hacked password. You may have received an email from Judy with a PDF attached — this message was not intended to be sent by us.

We have since updated our credentials and do not believe any personal or confidential information was exposed. We apologize for this breach and are committed to ensuring it doesn't happen again. To help you stay protected, please review the guide below.

WHAT IS PHISHING?

A scam where attackers impersonate a trusted source — a bank, IT team, or colleague — to trick you into clicking a link, entering credentials, or revealing sensitive data.

COMMON FORMS

Email phishing, SMS smishing, voice vishing, and spear phishing — targeted attacks using your name or role. Each mimics a real source to earn your trust quickly.

WHY IT WORKS

Phishing messages create urgency ("Your account will be suspended!") or authority ("This is HR") to pressure you into acting without thinking critically.

HOW TO SPOT IT

- | | |
|---|---|
| ■ Sender address doesn't match the organization | ■ Suspicious or mismatched links (hover to preview) |
| ■ Urgent or threatening language | ■ Spelling errors or unusual formatting |
| ■ Unexpected request for login or payment info | ■ Unexpected attachments, especially .zip or .exe |
| ■ Generic greeting ("Dear Customer") | ■ Too-good-to-be-true offers or prizes |

WHAT TO DO WHEN YOU SUSPECT PHISHING

STOP & VERIFY

Don't click any links.
Contact the sender
through a known, trusted
channel to confirm the
message is real before
taking any action.

REPORT IT

Forward phishing emails
to your IT or security
team. Most email clients
also have a built-in
"Report Phishing" button.

IF YOU CLICKED

Disconnect from the
network, change your
passwords immediately,
and notify IT right away.
Fast action limits the
damage.

Keep an Eye on Your Cameras

Your cameras work around the clock so your business doesn't have to worry — but a few minutes of regular care keeps footage sharp and your system ready when it matters most.

MONTHLY — 5 MIN PER CAMERA

- Clean lenses with a soft microfiber cloth — avoid paper towels.
- Check each view for new blind spots: branches, shelves, cobwebs.
- Inspect housings for cracks, condensation, or loose mounts.
- Confirm night vision is working after dark.

QUARTERLY

- Spot-check recordings for sharpness, correct timestamps, and audio.
- Test motion alerts by walking through the frame.
- Verify storage is saving correctly and space is available.
- Tighten any loose mounts or cables.

EVERY 6-12 MONTHS

- Update firmware to patch security vulnerabilities.
- Change passwords and enable two-factor authentication.
- Review user access — remove anyone who no longer needs it.
- Book a professional inspection to catch what you can't.

WARNING SIGNS TO ACT ON NOW

- Grainy footage or cameras dropping offline unexpectedly.
- Gaps in recordings or flickering night vision.
- Unusual login activity on your camera system.
- Small issues become big problems fast — don't wait.