Inbox Imposters!

Clues to Detect Phishing Before You Click.

Looks like
it's from Microsoft.

It's a phishing scam.

REINTIVITY
technology solutions

One click
could mean:

- **Breached** accounts
- **Stolen** data
- **Ransom** demands

All from **a fake email.**

Here’s how to spot the warning signs so your business stays safe.

REINTIVITY
technology solutions

Red flag
#1

Suspicious sender

The name looks right... but the email?

`alerts@security-m1crosoft.com`
Is that a “1” instead of an “i”?
Always check the full address.

Red flag
#2

Worrying links

"Click here to secure your account". **But the link goes to a strange site.**

Hover to check before you click.

REINTIVITY
technology solutions

Red flag
#3

Urgent language

*"This is your **FINAL WARNING**"*

Scammers want panic.
Pause a second.
Look closer.

Red flag

#4

Sloppy mistakes

Typos.
Blurry logos.
Weird formatting.

Big brands don't send messy emails

REINTIVITY
technology solutions

Red flag

#5

Asking for passwords

No legit company will ask for passwords by email. ***EVER.***

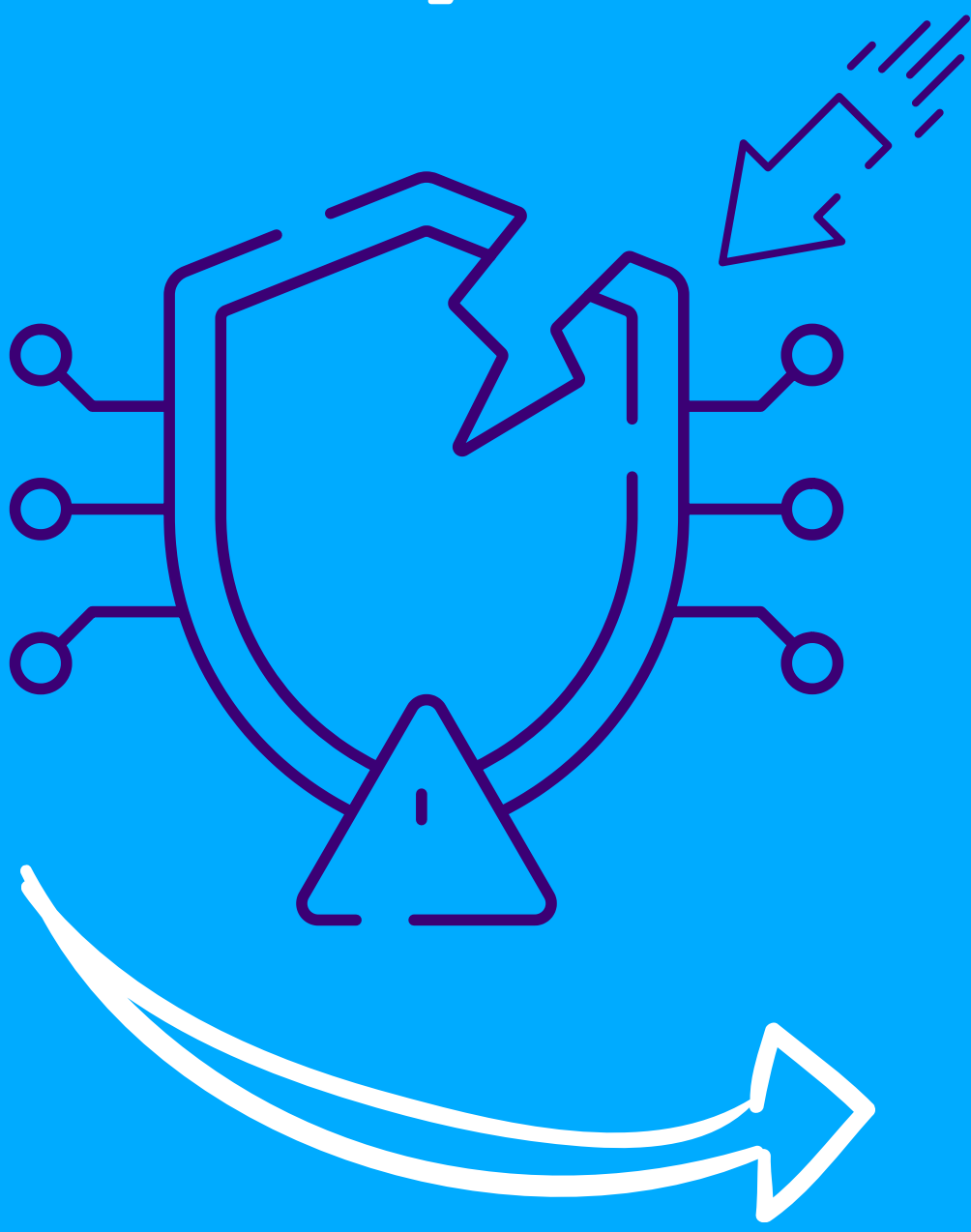
These scams are getting smarter.

Train your team to pause, check, and question before clicking.

REINTIVITY technology solutions

Knowing

what to look for
can protect your business from a costly attack.



Worried your team might fall for a phishing scam?

We can help.
Get in touch.

REINTIVITY
technology solutions