

LET'S MAKE IT HARDER FOR THEM

Is This Email Really From Them?

The 60-Second Impersonation & Domain Spoofing Checklist

Which one would you trust?

Fictional example domains

- | | | |
|-------------------------------------|---|---|
| ☒ | billing@acmecorp.com | The real domain: acmecorp.com |
| ☒ | billing@acmec0rp.com | A zero in place of the letter o |
| ☒ | billing@acmecorp-payments.com | A different domain: acmecorp-payments.com |
| ☒ | billing@acmecorp.secure-payments.com | The real domain is secure-payments.com |

Your brain recognizes brands. **Attackers count on you not reading domains character by character.**

BEFORE YOU CLICK, REPLY OR PAY

- | | |
|---|--|
| ☐ Check the full sender address
Ignore the display name. Expand the actual address. | ☐ Read the domain backwards
What matters is the registered domain—not the familiar-looking word somewhere in front of it. |
| ☐ Look for substitutions
0 for o, rn for m, added hyphens, missing letters and unexpected words. | ☐ Hover before you click
Does the destination match the organization you think you're visiting? |
| ☐ Question unusual urgency
"Do this immediately" + "don't call me" deserves extra scrutiny. | ☐ Ask: Is this normal behavior?
Even a perfectly written email can contain a request the supposed sender would never normally make. |
- ☐ **Verify consequential requests elsewhere**
Use a phone number, Teams/Slack conversation or contact information you already trust—not information supplied in the email.

ALWAYS VERIFY THESE REQUESTS



Banking changes • Wire transfers • Payroll/direct deposit • MFA resets • Password requests • Sensitive files • Gift cards • Changes to vendor payment instructions

WHEN IN DOUBT

STOP → VERIFY → REPORT



ishift.net



Scan for our security page

How Hard Are You to Impersonate?

A 2-minute external identity security check

Give yourself one point for every box you can honestly check. There are 16 in total.

01 PROTECT YOUR DOMAIN

- ☐ SPF is correctly configured
- ☐ DKIM signs outbound mail
- ☐ DMARC is implemented
- ☐ DMARC has progressed to enforcement
- ☐ Unauthorized sending sources are monitored

Remember: DMARC protects yourcompany.com. It doesn't stop someone from registering yourcompany-payments.com.

02 PROTECT YOUR IDENTITY

- ☐ Lookalike domains are monitored
- ☐ Newly registered domains resembling your brand are detected
- ☐ Common typo/homoglyph variations are monitored
- ☐ High-risk defensive domains are registered
- ☐ There is a process for investigating/taking down malicious domains

03 PROTECT THE TRANSACTION

- ☐ Banking changes require independent verification
- ☐ High-value transactions require dual approval
- ☐ Vendor payment changes cannot be authorized by email alone
- ☐ MFA/help-desk reset procedures address social engineering
- ☐ Employees can report suspicious messages easily
- ☐ Finance, HR and executives receive role-specific training

SCORE	WHAT IT MEANS
13–16	Hard Target Strong fundamentals. Keep testing them.
8–12	Attack Surface You've closed some doors, but important gaps remain.
0–7	Easy Wins Attackers have too many ways to borrow your identity.

LET'S MAKE IT HARDER FOR THEM.

You don't have to wait for someone to impersonate your company to find the gaps. iShift can help you assess your external security exposure, email security controls and the paths attackers are most likely to exploit.

[Talk to iShift →](#)

ishift.net/services/cybersecurity



Scan to connect