Mail Display Name Spoofing

Mail Display Name Spoofing is a trick used by cybercriminals to make an email look like it's from someone you know or trust. They change the name that appears in the "From" field of the email, but the actual email address is different. For example, you might get an email that looks like it's from your boss, but the email address is not your boss's real address. This tactic is often used to trick people into sharing sensitive information or clicking on malicious links. It's especially effective on mobile devices where you might only see the display name and not the full email address.

Here's a step-by-step breakdown of spoofing works:

1. **Selecting the Target:** Cybercriminals identify a target, often an organization or individual whose reputation or trustworthiness they can exploit.
2. **Creating a Spoofed Email:** The attacker creates a convincing email, using logos, formatting, and language that look like the real organization or person they're pretending to be.
3. **Manipulating the Display Name:** Instead of changing the email address, which can be easily detected, the attacker changes the sender's display name to match that of the trusted source. For example, they might change "John Doe " to "John Doe ."
4. **Sending the Email:** The cybercriminal sends the email to the target, who sees only the spoofed display name and not the actual email address.
5. **Deceptive Subject Line:** To further enhance the illusion, the attacker may use a subject line that instills urgency or curiosity, encouraging the recipient to open the email.

Why is it effective?

1. **Appearance of Legitimacy:** Recipients often trust emails that appear to come from familiar names or organizations, making them more likely to engage with the message.
2. **Minimal Technical Skill Required:** Spoofing a display name is relatively easy, even for less technically skilled attackers.
3. **Lack of Awareness:** Many email users are unaware of this technique and may not scrutinize the sender's details closely.

Protecting yourself

1. **Verify Email Addresses:** Always check the sender's full email address, not just the display name. If something seems off, don't open the email.
2. **Be Cautious of Urgent Messages:** Be skeptical of emails that demand immediate action or contain urgent requests. Cybercriminals often use urgency to pressure recipients into making hasty decisions.
3. **Hover Over Links:** Before clicking on any links within an email, hover your cursor over them to see the actual URL. If it looks suspicious, don't click it.
4. **Use Email Authentication Protocols:** Organizations can implement email authentication protocols like SPF (Sender Policy Framework) and DKIM (DomainKeys Identified Mail) to help prevent spoofing.
5. **Enable Multi-Factor Authentication (MFA):** Enabling MFA adds an extra layer of security to your email account, making it more challenging for attackers to gain access.
6. **Educate Yourself and Others:** Stay informed about email security threats and educate your colleagues and friends about the risks of mail display name spoofing.

Conclusion: Mail display name spoofing is a trick that can fool even careful email users. By learning how it works and following email security tips, you can protect yourself and your organization from this type of cybercrime. Stay alert, verify emails, and educate yourself to defend against email impersonation and spoofing.