# SCL -1: The Dangerous Side of Safe Senders

aon.com/cyber-solutions/aon_cyber_labs/scl-1-the-dangerous-side-of-safe-senders/

Stroz Friedberg is regularly called upon by clients to perform Business Email Compromise (BEC) investigations when their Microsoft 365® ("M365") tenants are compromised by threat actors. In the past few months, Stroz Friedberg has observed threat actors leveraging Safe Senders, a feature built into Outlook®, to bypass spam filters and successfully deliver spoofed messages to a targeted user's mailbox. These spoofed messages are altered to appear as if they originated from a specific email address, when the message was not actually sent from that address.

This article explores how the Safe Senders feature may be used legitimately, how it can be misused to create more advanced phishing emails, and how cybersecurity professionals can help to identify its illegitimate use. With the use of real-life scenarios and suggestions for targeted analysis, this article seeks to introduce cybersecurity professionals to this new technique and provide guidance on how to better recognize it in future incidents.

## Safe Senders Lists

Outlook Safe Senders is a feature that allows a user to add specific senders or domains to a list of senders whose emails "are never treated as junk email, regardless of the content of the message". In other words, Safe Senders allows messages coming from specific addresses or domains to skip spam filtering and land directly into a user's inbox. You may be familiar with this after having seen certain companies recommend that you add their address to your Safe Senders list. This has been seen as a more common practice among email marketers. When used legitimately, Safe Senders does allow a company to reach their customers more effectively. However, it can have significant security consequences when used illegitimately.

The ability to let messages bypass spam filtering can expose users to sophisticated phishing attacks that would otherwise have landed in their Junk folder. This does not mean that *all* messages from Safe Senders skip spam filtering; Microsoft documentation states that using Safe Senders "creates a high risk of attackers successfully delivering email to the Inbox that would otherwise be filtered; however, if a message from an entry in the user's Safe Senders or Safe Domains lists is determined to be malware or high confidence phishing, the message will be filtered". While high-confidence spam will still be filtered even if coming from a Safe Sender, a threat actor can easily adjust their strategy to ensure that their message does not get filtered as high-confidence spam. This has a couple notable implications for the security of M365.

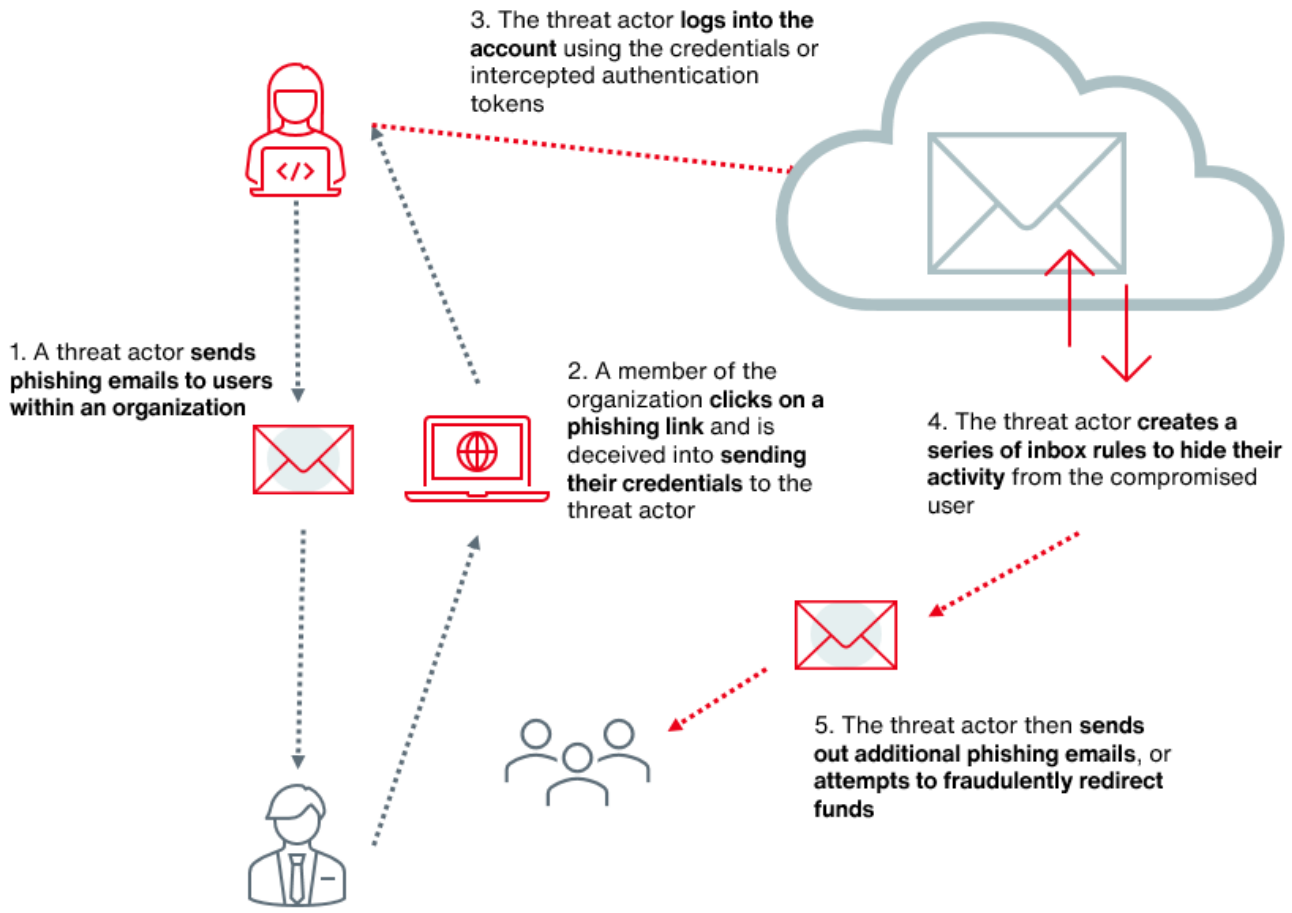
First, it makes BEC more effective. It can allow a threat actor to deliver a spoofed message that appears to be from a trusted partner to a victim's mailbox.

Second, any changes made to a victim environment can be leveraged at a later point in time by the threat actor if not detected and remediated by the organization. Companies should audit Safe Senders lists and the similar functions described below, not only as a part of their incident response process, but also as a part of regular audits of their M365 tenant outside the context of an incident. Otherwise, a threat actor that is evicted can regain their access using these methods to send additional spoofed emails that bypass standard spam filtering.

Other methods of bypassing spam filters are listed in Microsoft documentation. These methods include adding entries to the tenant Allow/Block list, creating tenant-wide transport rules, adding IP addresses to the IP Allow List, and adding entries to the allowed sender/domain lists. These methods differ from adding to a user's Safe Senders list because they require administrative permissions within the tenant, while Safe Senders lists are user-specific and only require access to a user's mailbox.

## Standard BEC Attack Pattern

Standard BEC incidents typically follow a similar pattern:



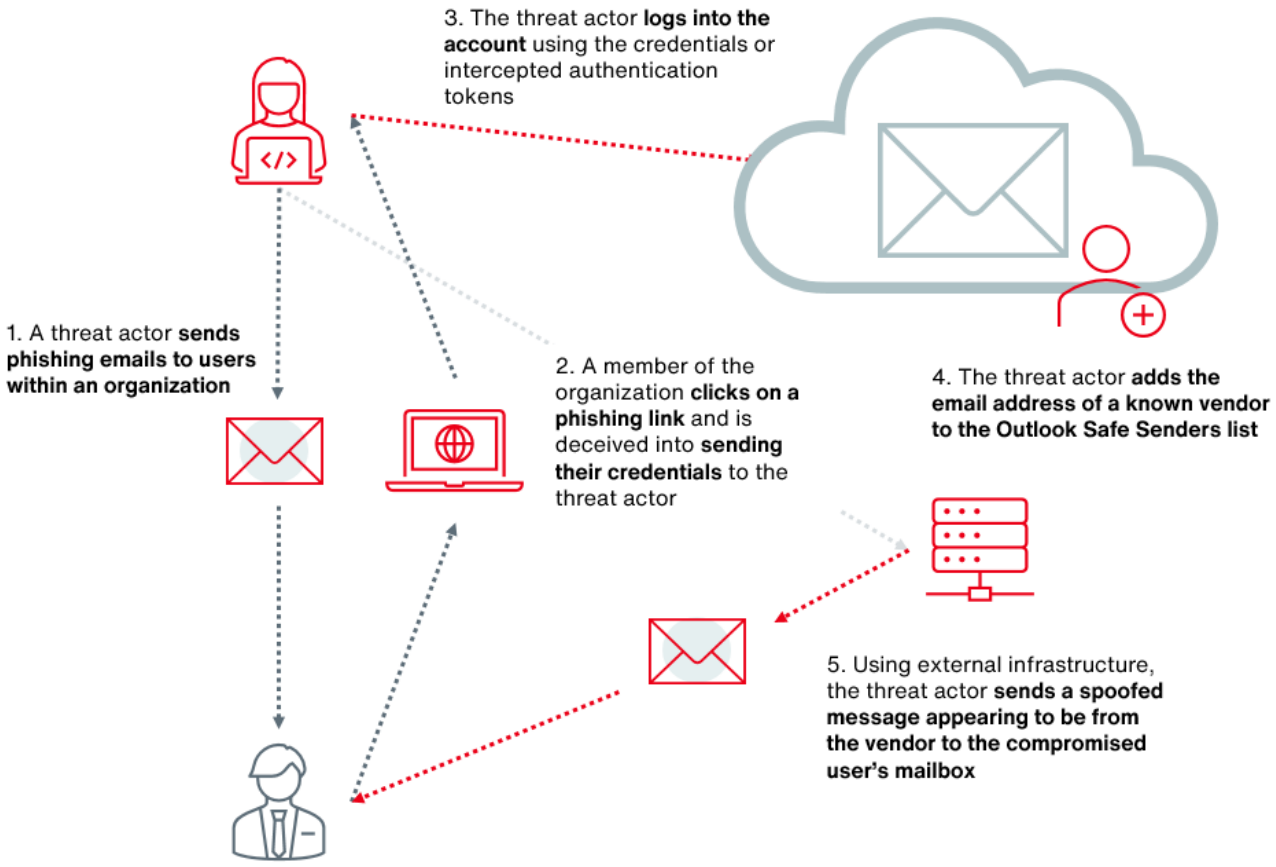
The use of Safe Senders allows threat actors to change this approach. The following scenario explains how this new technique may look to a cybersecurity professional investigating the incident and how it can change the attack pattern for threat actors performing Business Email Compromise.

## Safe Senders BEC Attack Pattern

Imagine you oversee the information security department at your company. You have been asked to lead an investigation into a fraudulent wire transfer initiated by someone in the accounting department. Everyone at your company has gone through multiple cybersecurity awareness trainings, so this comes as a surprise.

You start analyzing your company's M365 tenant and the mailbox of the user who initiated the wire transfer. You find that the message relaying fraudulent wire transfer information had failed standard authorization checks but was still successfully delivered to the user's mailbox. By all accounts, your spam filter should have caught this message. So how did the message reach the targeted user?

In this scenario, the threat actor used Safe Senders to functionally "allowlist" their spoofed sender address. The attack pattern of a Business Email Compromise leveraging Outlook Safe Senders looks like this:



From a threat actor's perspective, the difference in attack pattern is obvious. However, a cybersecurity professional may need to perform deeper analysis to identify when a threat actor has leveraged Safe Senders to bolster their phishing attacks. The following sections describe sources of information that an examiner should use to determine the use of Safe Senders in their next BEC investigation.

## Email Header Analysis

When performing email header analysis on suspicious messages, analyze the following headers:

- Failed or unknown authentication checks on messages in the user's inbox such as:
  - *dmarc=none* or *dmarc=fail*
  - *spf=none* or *spf=fail*
  - *dkim=none* or *dkim=fail*
  - *compauth=fail*
- Mismatched domains between smtp.mailfrom and header.from
- Mismatched X-Sender and Reply-To addresses
- X-MS-Exchange-Organization-SCL: -1

  A Spam Confidence Level (SCL) of -1 indicates that the message bypassed spam filtering
- X-Forefront-Antispam-Report: containing the values "SFV:SFE" "SFV:SKA" "SFV:SKI" or "SFV:SKN"

  Documentation of these headers can be found here.

Note that these header values may be present in legitimate emails, but given situational context they can also be an indication to investigate further.

## Unified Audit Log Analysis

To help identify the addition of items to the Safe Senders list when analyzing the Unified Audit Log, look for *Set-MailboxJunkEmailConfiguration* events. Stroz Friedberg's testing has identified slight differences in how these events appear in the logs based on whether the Safe Senders list was modified using PowerShell or Outlook on the Web (OWA). When added via PowerShell, the logs showed only the new address. Additions to the Safe Senders list via OWA, however, contained the entire Safe Senders list with the new address at the beginning of the list.

Parameters


```
[
    {
        "Name": "Identity",
        "Value": "[redacted].onmicrosoft.com"
    },
    {
        "Name": "TrustedSendersAndDomains",
        "Value": "+added_with_ps@gmail.com"
    }
]
```


*UAL-logged event of Safe Sender addition via PowerShell*

Parameters


*UAL-logged event of Safe Sender addition via OWA*

## Auditing the current state of a tenant

To audit the current state of your M365 environment using PowerShell, use the following commands:

To view the Safe Senders and Domains for a given user, you can use the following Exchange Online PowerShell command:

```
(Get-MailboxJunkEmailConfiguration [UserID]).TrustedSendersAndDomains
```

To view the tenant Allow/Block list, you can use the following Exchange Online PowerShell command:

```
Get-TenantAllowBlockListItems
```

To view the organization-wide IP Allow list, you can use the following Exchange Online PowerShell command:

```
(Get-HostedConnectionFilterPolicy).IPAllowList
```

To view the allowed sender/domain list along with other organization-wide anti-spam policies, you can use the following Exchange Online PowerShell commands:

```
(Get-HostedContentFilterPolicy Default).AllowedSender
```

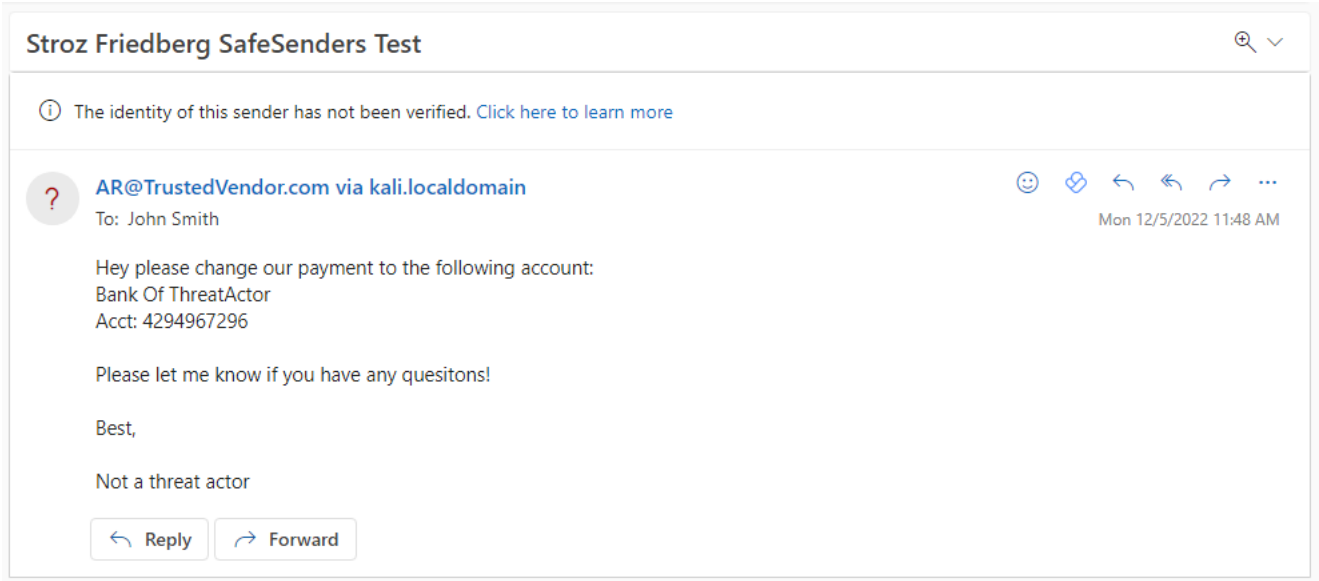
```
(Get-HostedContentFilterPolicy Default).AllowedSenderDomains
```

## Spoofed Messages from the User Perspective

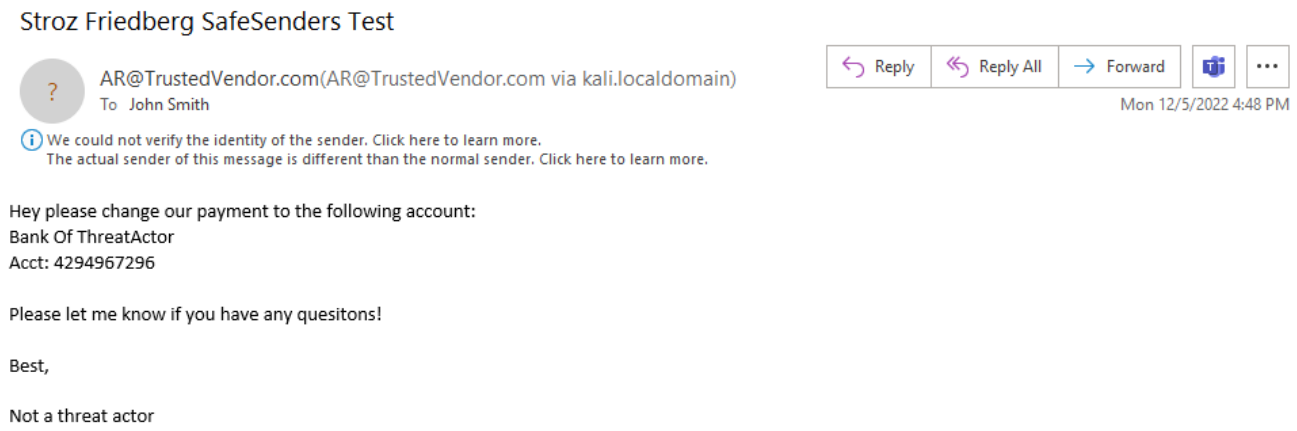
Stroz Friedberg tested the following three versions of Outlook to observe how they render spoofed messages received from Safe Senders:

1. OWA
2. Outlook 2016
3. Outlook 2021

In OWA and Outlook 2021, Microsoft alerts the user when a message is coming from a spoofed sender address. The screenshots below show the alerts rendered in OWA and Outlook 2021:

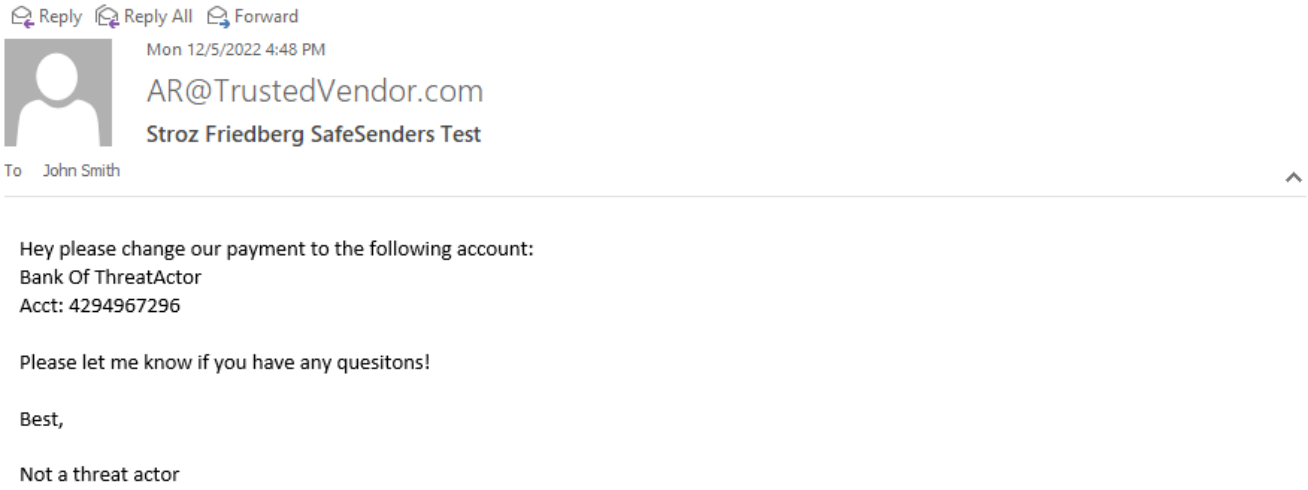



*Spoofed message viewed in OWA*




*Spoofed message viewed in Outlook 2021*

However, when rendering this same message in Outlook 2016, Microsoft does not alert the user about the spoofed sender address [1]:




*Spoofed message viewed in Outlook 2016*

Those using an old version of Outlook will have a much harder time identifying spoofed messages. Organizations should both encourage and ensure that updates to relevant software are done in order to take advantage of the most recent security features.

Organizations should also establish process controls requiring out-of-band confirmation of changes to payment information. It is possible that using a third-party spam filter in addition to Microsoft's built-in functionality may prevent messages from an address on the Safe Senders list from reaching a user's mailbox [2].

Threat actors are constantly coming up with new ways to abuse existing features on trusted platforms to bolster their attacks — staying aware of these patterns will help you identify and stop them as soon as possible.

*Authors: John Ailes, Julia Paluch*
December 16, 2022

This material has been prepared for informational purposes only and should not be relied on for any other purpose. You should consult with your own professional advisors or IT specialists before implementing any recommendation or following the guidance provided herein. Further, the information provided and the statements expressed are not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information and use sources that we consider reliable, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. The examples provided in this article are not based upon an actual Stroz/Aon client, but was provided for illustrative purposes only.

**About Cyber Solutions**
Cyber security services are offered by Stroz Friedberg Inc., its subsidiaries and affiliates. Stroz Friedberg is part of Aon's Cyber Solutions which offers holistic cyber risk management, unsurpassed investigative skills, and proprietary technologies to help clients uncover and quantify cyber risks, protect critical assets, and recover from cyber incidents.

1 Stroz Friedberg did not perform testing on how to prevent Outlook from displaying these alerts.

2 Stroz Friedberg did not perform testing on third-party spam filters. If a threat actor has sufficient privileges within M365, there may be other methods they could use to bypass third-party spam filtering solutions.


Cyber security services offered by Stroz Friedberg Inc. and its affiliates. Insurance products and services offered by Aon Risk Insurance Services West, Inc., Aon Risk Services Central, Inc., Aon Risk Services Northeast, Inc., Aon Risk Services Southwest, Inc., and Aon Risk Services, Inc. of Florida and their licensed affiliates. Aon UK Limited is authorised and regulated by the Financial Conduct Authority in respect of insurance distribution services. FP.AGRC.238.JJ The following products or services are not regulated by the Financial Conduct Authority:
• Cyber risk services provided by Aon UK Limited and its affiliates
• Cyber security services provided by Stroz Friedberg Limited and its affiliates.