OFFICE 365
MAIL FILTERING BEST PRACTICES

SPRING 2022

BITLYFT CYBERSECURITY
BITLYFT.COM

OFFICE 365 BEST PRACTICES

The following is a collection of Office 365 mail flow rule configurations that will help you reduce spam and phishing attempts on your organization. These are starting recommendations we've gathered through extensive field work across multiple client environments to help keep them more secure.

US-Cert O365 Recommendations

https://www.us-cert.gov/ncas/alerts/aa20-120a

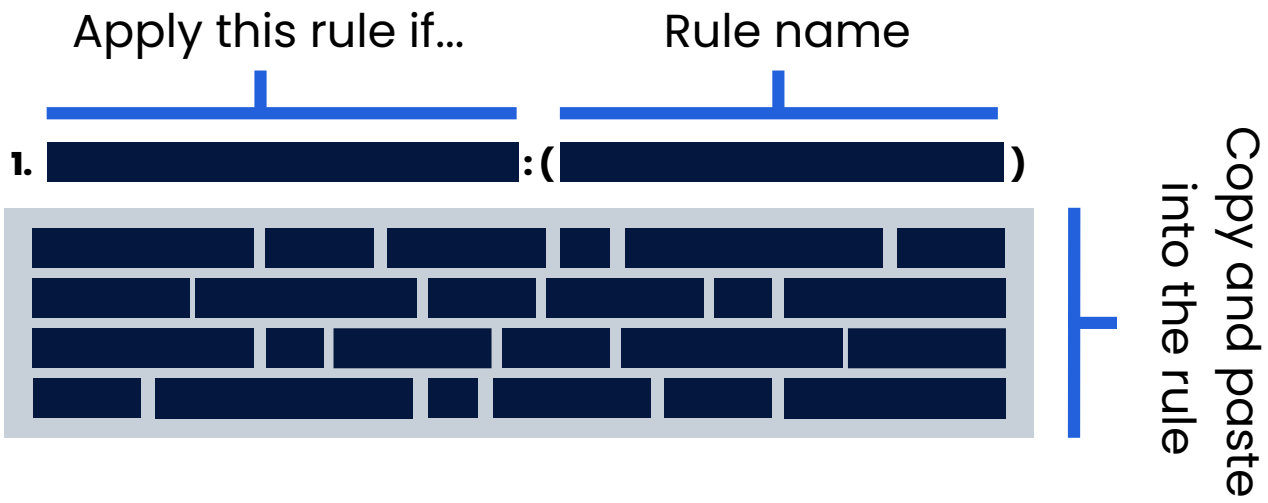
- MFA - Turn on “Security Defaults” for MFA on Azure AD Global Admin accounts, turn on for all accounts if possible.
- Role Based Access Control - Use lease privileged accounts, especially when it comes to using the Global Admin account.
- Unified Audit Log - Turn on in Security and Compliance Center so allow for queries.
- Legacy Protocols - Turn off POP3, IMAP, and SMTP, use Conditional Access if you must keep them around.
- Turn on Alerts for Specific Activity in Security and Compliance Center. Minimum enable logins from suspicious locations and email thresholds, may require some tuning.
- Microsoft Secure Score - Turn on to get Dashboard for security posture and keep up with changes
- Integrate Logging with SIEM - Because SIEMs are great for gathering and analyzing log data.

BitLyft Additional Recommendations

- External sender banner (RED)
- SPF, DKIM, and DMARC hardening (docs provided)
- Mail filtering products like https://abnormalsecurity.com, https://www.avanan.com
- phishing campaign tools like https://www.knowbe4.com
- remove legacy accounts that have no business with your school/company (move to different domain)
- separate domains faculty / students
- add Exchange mail flow rules, continue to update when new events take place (these are limited in number of rules allowed but care and feeding will help to limit repeats)

How to use this guide:

To properly utilize this guide you will need to have access to the **Microsoft Exchange Admin Center**. Navigate to the **mail flow rules** tab, and create a new rule. The first part of the title of each section (i.e. if the sender address includes) will be the "apply this rule if... section". Inside the brackets is the naming convention that we chose for the rule. The gray box is what you will copy and paste into the rule. Our recommendation is to **block all messages that break these rules**.



1. if the sender address includes: (Custom black list)

'lsaspac.com' or 'awntx3.email.active.com' or '\.xyz' or 'wizorh.org' or '@mailinator.com' or '.xyz' or 'fb@fb.com' or 'affordableclaim.icu' or 'chair.department@gmail.com' or 'office-365@sec' or 'suzanne@apsact.com.au' or 'noreply@gotinder.com' or 'hr@humanresources.com' or 'gubarevae@yahoo.com' or 'ucertify.com' or 'mieke@kleinekompagnie.be' or 'elearning040@gmail.com' or 'ticket@noahmanko.com' or 'nhs.net' or 'ye@gmail.com' or 'crooksrichard57@gmail.com' or '@morning7.theskimm.com' or '@dimepsa.com' or 'msg.sser@ms.offceonline.com' or 'euronursing@innovinc.org' or 'worldnursing@innovinc' or 'kenmello@ecwcesmail.com' or 'volimm.trade' or 'fotf.com' or 'judicialwatch.org' or '@verify.edu' or 'bchict.com' or '@mediatransport.com' or 'rockshores@yahoo.co.uk' or '@24.com' or '@mail12.suw15.mcsv.net' or 'felver2011@gmail.com' or '@grafe-dran.com' or '@jhs.co.uk' or '@cashpro.com' or '@fax-your.com' or '@efax.com' or '@fax-global.com' or '@my-fax.com' or '@invoice.com' or 'email.tmart.ru'

2. if attachments contain the following: (attachment scanner)

'ATT84666.htm' or 'PaperWork.html' or 'jkhgdfs.ginnonline.com/saint.php' or 'http://jkhgdfs.ginnonline.com/saint.php'

3. attachment file extension matches: (Small Attachment Redirection)

'jar' or 'slk' or 'msi' or 'cmd' or 'chm' or 'bat' or 'vbs' or 'exe'

*and attachment is greater than or equal to '0.00 KB' will need exclusions in place as well.

4. the subject or body includes: (fake online orders or hotels or spamming)

'tcoin' or 'contribution will bring improvement' or 'secured document with your school login' or 'bitcoin' or 'Employee Evaluation Report' or 'Bitcoin wallet' or 'btc purse' or 'ATM card number' or 'I know your password' or 'usd in bitcoin' or 'MASTER CARD IS READY' or 'recruitment exercise for retail survey' or 'Confirm Your Interest & APPLICATION' or 'mystery shop' or 'SmartSerialMail' or 'goo.gl/Gg4jw1' or 'tracking and further information kind' or 'has been delivered to your local FedEx' or 'duratrade.net' or 'amazons.com' or 'usintecmedical.com.br' or 'bofa_card_statement_' or 'We are grateful for your purchase from our shop and' or 'hey! perfect article!' or 'https://docs.google.com/a/sheridanschools.org/spreadsheet' or 'Amazon.com order of Panasonic UN55EH7070 55-Inch' or 'See our Returns Policy or contact Customer Service Walmart.com Total: $960.86' or 'http://www.armadillocentral.com/' or 'http://giatanmedia.net/' or 'complains.walrnartmail.com' or 'Your reservation at HOTEL UNION SQUARE'

5. the subject or body matches: (generic spam list)

'fucked' or 'fucking' or 'firebasestorage' or 'pet sitter' or 'Integrity program is attached' or 'mance Based Increase' or 'btc wallet' or 'masturbating' or 'supplied with key logger' or 'erase this compromising' or 'playing with yourself is' or 'adjusted virus on a web' or 'my victim' or 'fuck ' or 'awesome sex' or 'hot nudes' or 'hunger for sex' or 'innovincconferences' or 'migrating all email' or 'go2l\.ink' or 'radhaus\.ca' or 'Seeks interested candidates to go' or 'Firma Bank Payment' or 'nude pic' or 'naked pic' or 'bare flirty photo' or 'hot nude body' or 'dential documents with you via google' or 'look your attached document' or 'Look the documen ' or 'milk worse than smoking'

6. sender is located outside the org and subject or body matches (fake file recieved)

'received a new file' or 'www\.surveygizmo\.com' or 'file shared' or 'Irregular Activity' or 'Incoming Messages'

7. subject or body matches: (fake encrypted message)

'received a secured doc' or 'support centre has sent' or 'office-365 team' or 'is the secure email' or 'NHSmail is approved' or 'You have a new encrypted' or 'view the secure'

8. the subject or body matches: (more fake email updates)

'pending messages' or 'undelivered clustered' or 'indefinitely revoked' or 'incoming mails' or 'transitioned from Microsoft' or 'Submit to update' or 'messages were affected' or 'Office365 team' or 'mails undelivered' or 'Protected Messages' or 'sent using One' or 'shared a file' or 'retrieve some pending' or 'share some files' or 'secured-drpbox.com' or 'got a new document' or 'deawb.org' or 'avoid mail malfunction' or 'confirm your email password' or 'Message from Univer' or 'do ument was shared via One' or 'important unread message' or 'document waiting' or 'sent to you via One' or 'terminate reset password' or 'credentials is listed to be reset' or 'Web-mail Update' or 'our newly updated Web' or 'update your Webm' or 'click on the link Outlook' or 'secure your account' or 'gain access into your' or 'suspension of your' or 'account unusual sign' or 'Unread Messages from the Stu' or 'warning and your request' or 'email will be closed shortly' or 'terminate your account' or 'instruction few hours ago to term' or 'regarding mailbox upgrade' or 'several negligence of emails' or 'account will be shut down' or 'Sincerely, Help Desk' or 'Kindly confirm that your account' or 'Help Desk Notice' or 'help desk survey on your email' or 'IS THIS EMAIL STILL ACTIVE' or 'I have been trying to reach you contact' or 'Subject to mandatory upgrade' or 'Permanent closure of your acc' or 'kindly click on the link below' or 'mail account was login today by Un' or 'login to validate and verify your e' or 'failure to update your email' or 'Verify your Personal identity to re' or 'upgraded to our new mailbox space' or 'upgraded our mailbox s' or 'mail User authentication form' or 'mail has been improved this' or 'still open for you to send and r' or 'Please login to your account to validate E' or 'has currently upgraded all mailboxes' or 'upgrade your account now to avoid' or 'We noticed seizure on your mails' or 'update that our new webmail' or 'access link below to complete your u' or 'provide the requested details on the link b' or '<your name>\.890m' or 'low mail quota' or 'currently upgraded to 4GB' or 'mailbox quota size increase in progress' or 'wait for response from Webmail' or 'after which restart your device/c' or 'login again with your email info' or 'ATM Card payment $1.5 Million USD' or 'updateoutlookwebaccount' or 'Security Center is shutting down some accounts' or 'worth US$10.5M'

9. the subject or body includes: (fake mailbox quota or security upgrades)

'Critical Microsoft Windows' or 'Install Latest Microsoft Windows Update now' or 'file has been shared' or 'share some files' or 'will expire today' or 'update their account' or 'around the <your name>' or '<your name> self' or 'provided by <yourname>' or 'Pass-word will expire' or 'File Was Sent To You Via One' or 'Please Update Your Payment Method Now' or 'sign in with a Mıcrosoft account to view the secured doc' or 'colleague has shared an important document' or 'account information require Update' or 'Invitation to view an Adobe Document' or 'Your Contact has invited you to view the following' or 'should fix any mailbox malfunctions' or 'Further messages might not be delivered' or 'update notification!' or 'pending messages from the Human' or 'ensure your email account stays validated' or 'CLICK TO UPDATE NOW' or 'exceeded its storage limit' or 'detailed resolution steps on how to resolve' or 'as Shared a file with you Using Onedrive' or 'Kindly find attached lookahead files' or 'iqramds.org' or 'All Staff members are required' or 'mailbox is almost full' or 'mailbox might be close' or 'documents via Microsoft Exchange Portal' or 'render your Outlook Web App account' or 'Failure to do this within the next 24 hours' or 'kindly click activate' or 'Your mailbox might be closed' or 'upgrade for our new Outlook Web Access' or 'New security updates need to be performed' or 'account will be deactivated to create space' or 'inactive if this survey is not completed' or 'Upgrade your mailboxes' or 'mail will expire soon' or 'Your Mailbox might be closed today' or 'confirm your email address' or 'avoid disconnection from our data base' or 'updateoutlookwebaccount' or 'Dear Staff and Employee Email Subscribers' or 'submit your old account for new to enable' or 'Your Email Account Have Put on' or 'your email account is up to date' or 'all email users are urged to update' or 'validate your mailbox' or 'To re-validate your mailbox please' or 'Your mailbox has exceeded' or 'Due to our latest IP Security upgrades we' or 'mailbox has exceeded it storage' or 'You are therefore required to re' or 'Your email account will be upgrade' or 'Roundcube - Free webmail for the masses' or 'We are upgrading our Webmail clients.' or 'validate your mailbox please click the link below' or 'Mail Service messaging center wish to inform' or 'edu Mail HelpDesk' or 'Your Email Will Expire in 24hours' or 'microsoft\-helpdesk\.net\.ms' or 'You will not be able to send' or 'Your mailbox has exceeded one or more size limits' or 'upgrade your email quota' or 'You have exceeded your mailbox' or 'mailbox quota storage limit'

10. subject or body includes: ($20 million proposal)

'pay your withheld' or 'unable to reach you with the payment' or 'Order Via ATM' or 'claim your Inheritance' or 'growing into a missional bill' or 'sharing of business profit' or 'Please grant me the benefit of do' or 'your benefit is fifty percent of' or 'selected for huge amount' or 'back to claim your Donation' or 'Global intelligence monitoring' or 'among the lucky individuals to benefit' or 'address was attached to a cash' or 'help to transfer my late husb' or '$20 Million Proposal'

11. subject matches: (multi subject)

'TIME JOB OPPORTUNITY' or 'ACTI0N REQUIRED\: BRAND AMBASSAD0R' or 'Memo From HR Department' or 'Job Referral'

12. subject or body includes: (blackboard fake notice)

'Please sign in immediately to confirm the update, ' or 'http://www.kiwasushi.com/wp-includes/js/crop/board3/blackboard.htm' or 'a new course has been added to your study list and also view your timetable'

13. the subject or body matches: (hello http spam! or Hey Cool site spam!)

'hello\! http' or 'hi\! http' or 'Excellent site http' or 'Super site http' or 'Perfect site http' or 'Outstanding site http' or 'Cool site http' or 'Awesome site http' or 'Have a look http'

14. subject or body matches: (fake robbed on trip message)

'meets your heartfelt considerations and any assistance rendered' or 'we got robbed at gunpoint' or 'Unfortunately I was mugged at gun point' or 'I was robbed of my cash' or 'I need you lend me some money, about $1,950 or whatever you can afford.' or 'had to be in Manilla Philippines for a program' or 'all I need is $1900 please let me know soonest.'

15. the subject or body contains: (custom URL blocklist)

'njci\.co\.za' or 'mailsecure9\.host' or '\.xyz' or 'cliffzone\.com'

16. subject contains: (fake faxes)

'New incoming fax' or 'Thank you for using the Fax' or 'View this fax using your PDF reader'

17. subject or body matches: (fake payment notification and blown up)

'credited to your bank a' or 'ACH payment slip' or 'device explodes' or 'is under my control' or 'Performance Based Increase' or 'regalconsult.com/j' or 'or be blown up' or 'pay up or be blown up' or 'per assignment which would come in the form' or 'Payment has been made for amount 21'

18. the subject matches: (update invoice)

'updated invoice'

19. subject or body matches: (fake payment notification and blown up)

'credited to your bank a' or 'ACH payment slip' or 'device explodes' or 'is under my control' or 'Performance Based Increase' or 'regalconsult.com/j' or 'or be blown up' or 'pay up or be blown up' or 'per assignment which would come in the form' or 'Payment has been made for amount 21'

20. the subject matches: (update invoice)

'updated invoice'

21. the subject or body includes: (your password expires today - fake)

'microsftonlnecom' or 'supportpezrm' or 'Password will expire in 2hour' or 'password policy requires that all' or 'Your Password Expires in 2 hours' or 'recent activities going on in your account' or 'your account has been temporarily disabled due to suspicious activity' or 'Your Password Expires Today, To Verifiy and' or 'any questions please contact the IT Helpdesk' or 'We currently upgraded our Server to 50GB inbox space' or 'i want to present you as a next of kin to my late' or 'Mr. Raymond picked you'

22. the subject or body matches: (fake job offer)

'Assistant Needed \(' or 'IWU Job opening' or 'make extra income' or 'Part time job openi' or 'great job openi' or 'students to work from hom' or '3hrs daily for two times' or 'Inc is currently searchi' or 'eager to learn with mini'

23. the subject or body matches: (copy of fake payment notification)

'failed to process your C' or 'microsoftonlnecom' or 'per assignment which would come in the form of a c' or 'Payment has been made for amount 21'

24. sender is located outside the org and subject or body matches: (do something for me urgently)

'Office E3 has been' or 'helpdesk service' or 'something for me urgently'