Installation Outline

INKY Installation for Office 365

The INKY Phish Fence installs on Office 365 utilizing 'Connectors' and 'Transport rules' in two 30-minute sessions. INKY will begin analyzing your mail and arming your end users with the information that they need to protect themselves against Phishing attacks.

Discovery

Basic Information needed before onboarding:

1. Domain: company.com
2. Domain Admin: user@company.com
3. Domain Tenant address: company-com.mail.protection.outlook.com
    a. Login to https://admin.microsoft.com/
    b. Click "Show all" if all the settings are collapsed
    c. Click "Setup" then select "Domains"
    d. Select the domain INKY is going to protect
    e. The tenant address will be in the MX record row and look like: domain-com.mail.protection.outlook.com

We like to run a discovery first which gives us an overview of how their O365 domain is set up. Then we run Phish Finder which shows us the last seven days of email to see how INKY would have scored the messages.

The Inky installer web tool cannot sign a user in using Multifactor Authentication. If a client's account has MFA enabled, one way to handle the situation is to use an app password with the web tool. An app password is a password that Office 365 can create for you, that is intended to be used with a single app that doesn't support MFA (this is just a convention; nothing technically ties the password to an app). To create and app password (this is copied from https://support.office.com/en-us/article/create-an-app-password-for-office-365-3e7c860f-bda4-4441-a618-b53953ee1183):

1. Go to https://inkypsdiscovery.azurewebsites.net/
2. Log in using the domain admin credentials
3. Click Discovery at the top left then Start
4. Next Click Phish Finder at the top right
    a. Then hit Create Groups
    b. Then click phisher finder at the top right again
    c. Then click Grant API Access – then click Yes on the Microsoft grant API access page
5. Once that is done go to the domain Exchange Admin Pages
6. Go to Groups and add inboxes to the IPW-Group-Discovery (around 20 maximum)
7. Go to the INKY dashboard at https://shared.outlook.inky.com/dashboard
    a. Select API Access
    b. Find INKY Groups

c. Click “Start Processing” on the IPW-Group-Discovery

Install Planning Call

Following the gathering of the information the INKY and Customer Teams will meet to review the finding and to review a proposed deployment plan. This call will only be needed if there is a lot of custom configuration on a tenant.

INKY will present findings made by the INKY Phish Finder tool and discuss any potential steps needed to mitigate any issues it may uncover. These may include recommendations for pre-launch changes to accommodate existing tools in mail ecosystem.

The Customer will provide a list of all email addresses of POV stakeholders that will be evaluating Phish Fence and identify which addresses on the list are going to be involved with Installation and subsequent configuration testing.

The Customer and INKY will coordinate to schedule the INKY installation in accordance with change management processes.

Installation - Launch Day

Verify completion of prerequisites. This includes reviewing that you know the users to include in the IPW-Group following installation and testing.

Install the INKY Phish Fence via the Web Installer or PowerShell if necessary. Both methods require an Office 365 account with administrative privileges for Exchange for the target domain:

1. Installation
2. **https://inkypsdiscovery.azurewebsites.net**
   i. Click Install
   ii. Click Start button
   iii. Generally, takes 3-5 minutes to install Transport Rules and Connectors
   iv. Add test user to the IPW-Group on the clients Office 365 Admin Page
3. **https://inkypsdiscovery.azurewebsites.net**
   i. Click Enable/Disable
   ii. Click Start Button
   iii. Generally, takes 1 minute to activate
4. **Allow Microsoft time to activate transport rules and connectors**
   i. Process takes between 5 and 30 minutes on average
   ii. Send test mails to the account added to IPW-Group earlier
   iii. When an Inky banner is observed we will know that processing is in place and rule activation is complete.
   iv. Reply to a test message to verify outbound banner removal is working properly.

5. **Setup is now complete, and you may populate the IPW-Group with users who will use the Inky Service**.
    i. You can nest groups including dynamic groups into the IPW-Group to simplify rollout.
    ii. If you have a specific user or users, you do not want processed by Inky you can add those users to IPW-Group-Exclude

You have completed INKY installation; INKY engineers will work with you to schedule a follow-up call in a few days to review how things are going and continue to customize INKY to your unique Email environment.

INKY always recommends that you follow email configuration and security best practices. If you would like help configuring SPF, DKIM and DMARC for your domain(s) we are happy to assist you. If you need help with the configuration of a new or existing 3rd party service that sends mail on behalf of your domain(s) we will work to assist and confirm your tools are sending mail correctly on your behalf.

Please review the INKY FAQ for the latest information from INKY on banners.