

How to Use Sniff and Detect

Overview

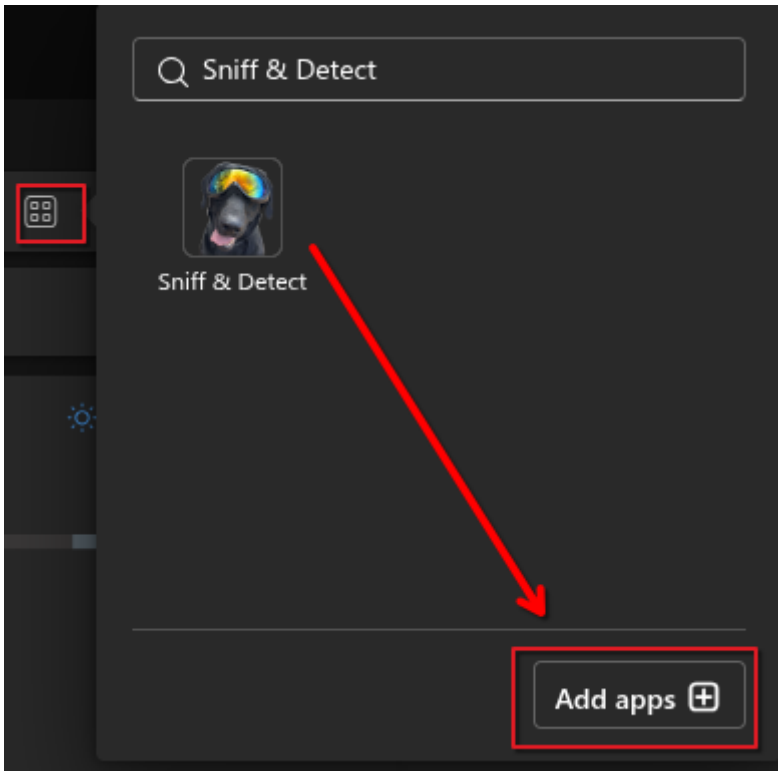
AQUILA – SNIFF & Detect is a custom integration app within the **AQUILA platform** that enables Microsoft 365 environments to deploy **advanced malicious email detection** capabilities. The app is packaged as a **manifest.xml** file and can be added to an organization’s Microsoft 365 tenant via the **Integration Apps** section in the Microsoft 365 Admin Center.

Key Capabilities & Value

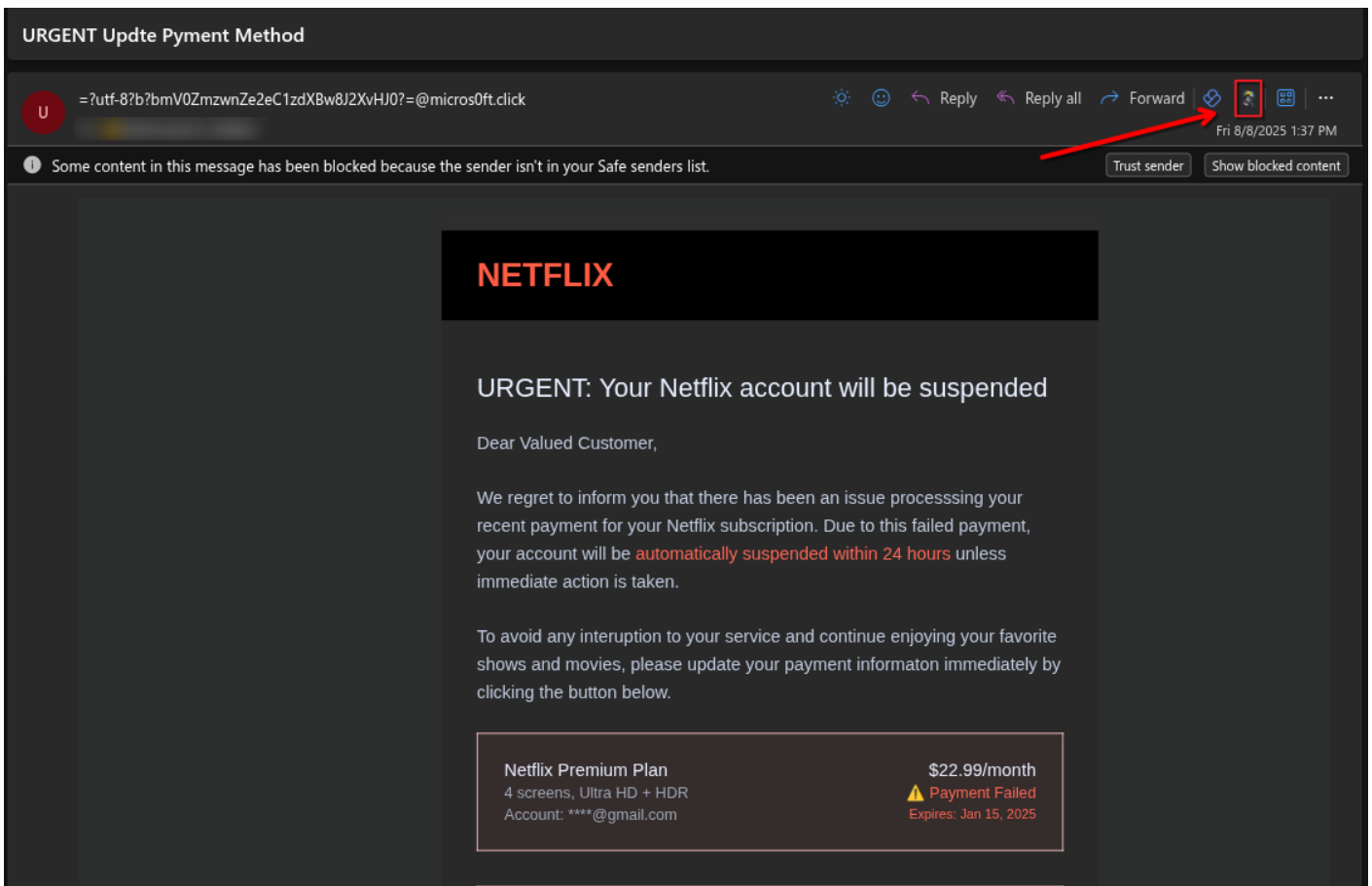
- **Seamless Integration** – Install in Microsoft 365 with just a few clicks, no complex infrastructure required.
 - **Permission-Driven Security** – Requires admin approval to grant permissions, ensuring a secure deployment process.
 - **Centralized Control** – Managed via AQUILA and distributed through the AQUILA Store for consistent updates.
 - **AI-Enhanced Detection** – Uses AQUILA’s AI and Cyber Threat Intelligence to scan and detect malicious emails in real time.
 - **User-Friendly Accessibility** – Appears in the “More apps” section for assigned users, making it easy to launch.
 - **Minimal Footprint** – Only ~6 KiB in size, ensuring fast installation without performance impact.
-

Simple Step-by-Step Instructions

1. **Access the App**
 - Open Outlook and check the apps panel to ensure Sniff & Detect is listed and accessible.
 - Users can launch it from **More apps** in Microsoft 365.






- A phishing email impersonating Netflix. An arrow points to the **SNIFF & Detect** icon, indicating where to scan or flag the email as suspicious.



- Click the **"Scan This Email"** button and wait for the scan to complete.

URGENT Updte Pymnt Method

 =?utf-8?b?bmV0ZmZwnZe2eC1zdXBw8J2XvHJ0?=@microsoft.click
To:  Richmond A. Abella Fri 8/8/2025 1:37 PM

 Some content in this message has been blocked because the sender isn't in your Safe senders list. [Trust sender](#) [Show blocked content](#)

NETFLIX


URGENT: Your Netflix account will be suspended

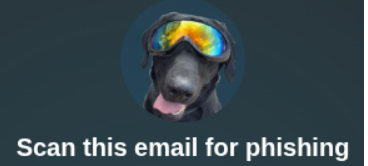
Dear Valued Customer,

We regret to inform you that there has been an issue processsing your recent payment for your Netflix subscription. Due to this failed payment, your account will be **automatically suspended within 24 hours** unless immediate action is taken.

To avoid any interruption to your service and continue enjoying your favorite shows and movies, please update your payment informaton immediately by clicking the button below.

Netflix Premium Plan
4 screens, Ultra HD + HDR
Account: ****@gmail.com




\$22.99/month
 **Payment Failed**
Expires: Jan 15, 2025



Scan this email for phishing

Scan this email for potential threats and receive actionable security insights and recommendations.

What does this do?

-  Analyzes email content, links, and attachments for threats
-  Provides security recommendations based on scan results
-  Offers detailed technical analysis for security teams

[Scan This Email](#)

- SNIFF & Detect has scanned the email, highlighting possible errors such as
 1. **Arrow 1** points to the **Language issues** section, showing spelling and grammar mistakes found in the phishing email.
 2. **Arrow 2** points to the **What you should do** section, giving safety advice on how to handle the suspicious email.

The screenshot displays an email client interface. The main email content is a phishing message from Netflix with the subject "URGENT: Your Netflix account will be suspended". The email body contains a warning about account suspension and a button to "Update Payment Method". A side panel titled "Sniff & Detect" provides AI insight results, including a "Malicious" classification and a list of language issues such as spelling and grammar errors. Two red arrows point from the side panel to the email content: Arrow 1 points to the "AI Insight Results" tab, and Arrow 2 points to the "Report as Phishing" button.

- **Arrow 1** - Highlights the **AI Insight Results** tab in SNIFF & Detect, which contains the automated analysis results of the scanned email.
- **Arrow 2** - Points to the **Malicious** classification summary. This section briefly explains the reasons the email is flagged, such as suspicious sender details, urgent tone, spelling and grammar errors, and suspicious links.
- **Arrow 3** - Directs attention to the actual phishing email content pretending to be from Netflix, warning about a payment failure and urging the user to update their payment information.
- **Arrow 4** - Indicates the **Report as Phishing** button, which the user can click to formally report the suspicious email to security for further action.

Read / Unread

URGENT Updte Pymment Method

=?utf-8?b?bmV0ZmzwnZe2eC1zdXBw8J2XvHJ0?=@microsoft.click

Fri 8/8/2025 1:37 PM

Some content in this message has been blocked because the sender isn't in your Safe senders list.

Trust sender Show blocked content

NETFLIX

URGENT: Your Netflix account will be suspended

Dear Valued Customer,

We regret to inform you that there has been an issue processing your recent payment for your Netflix subscription. Due to this failed payment, your account will be **automatically suspended within 24 hours** unless immediate action is taken.

To avoid any interruption to your service and continue enjoying your favorite shows and movies, please update your payment informaton immediately by clicking the button below.

Netflix Premium Plan \$22.99/month
4 screens, Ultra HD + HDR
Account: ****@gmail.com

Payment Failed
Expires: Jan 15, 2025

Sniff & Detect

AI Insight Results Deep Scan Results

AI Insight completed at October 26, 2023 16:13:11

Malicious

Suspicious sender details, urgent tone, spelling and grammar errors, and a suspicious link to update payment information.

AI-generated result.

Indicators found Malicious

- Sender email address does not match Netflix's official domain.
- Subject line contains spelling errors and urgency.
- The email body contains several grammatical errors and inconsistencies.
- The email threatens account suspension unless payment information is updated immediately.
- No secure link provided to update payment information; instead, a simple button is used.
- The 'Secure 256-bit SSL encryption' claim is generic and unsubstantiated.
- The email uses generic greetings and closings.
- The provided IP address (192.168.1.45) is a private IP address and not associated with Netflix.

Report as Phishing

Run a deep scan

Powered by AQUILA

- Click the **"Run a deep scan"** button, which allows for a more detailed examination of the email to detect hidden threats and malicious indicators.

Read / Unread

URGENT Update Payment Method

=?utf-8?b?bmV0ZmzwnZe2eC1zdXBw8J2XvHJ0?=@microso0ft.click

Fri 8/8/2025 1:37 PM

Some content in this message has been blocked because the sender isn't in your Safe senders list.

Trust sender Show blocked content

NETFLIX

URGENT: Your Netflix account will be suspended

Dear Valued Customer,

We regret to inform you that there has been an issue processing your recent payment for your Netflix subscription. Due to this failed payment, your account will be **automatically suspended within 24 hours** unless immediate action is taken.

To avoid any interruption to your service and continue enjoying your favorite shows and movies, please update your payment informaton immediately by clicking the button below.

Netflix Premium Plan \$22.99/month
4 screens, Ultra HD + HDR
Account: ****@gmail.com

Payment Failed
Expires: Jan 15, 2025

Sniff & Detect

AI Insight Results Deep Scan Results

AI Insight completed at October 26, 2023 16:13:11

Malicious

Suspicious sender details, urgent tone, spelling and grammar errors, and a suspicious link to update payment information.

AI-generated result.

Indicators found Malicious

- Sender email address does not match Netflix's official domain.
- Subject line contains spelling errors and urgency.
- The email body contains several grammatical errors and inconsistencies.
- The email threatens account suspension unless payment information is updated immediately.
- No secure link provided to update payment information; instead, a simple button is used.
- The 'Secure 256-bit SSL encryption' claim is generic and unsubstantiated.
- The email uses generic greetings and closings.
- The provided IP address (192.168.1.45) is a private IP address and not associated with Netflix.

Report as Phishing

Run a deep scan

Powered by AQUILA

- **SNIFF & Detect** doing a deep scan on a suspected phishing email pretending to be from Netflix. The scan may take a couple of minutes to finish.

The image shows an email client interface with a phishing attempt and a security scan sidebar. The email subject is "URGENT Updte Pymment Method". The sender is a Microsoft account. The email content includes a "NETFLIX" logo and a message: "URGENT: Your Netflix account will be suspended". The sidebar, titled "Sniff & Detect", shows "Deep Scan Results" with a "Caution During Scan" warning and a "Results" section. The "Results" section shows "Domains 0", "Email Adresse...", and "IP Address 0", all with "Scanning..." status. A "Report as Phishing" button is at the bottom of the sidebar.

Read / Unread

URGENT Updte Pymment Method

=?utf-8?b?bmV0ZmzwnZe2eC1zdXBw8J2XvHJ0?=@microso0ft.click

Fri 8/8/2025 1:37 PM

Some content in this message has been blocked because the sender isn't in your Safe senders list.

Trust sender Show blocked content

NETFLIX

URGENT: Your Netflix account will be suspended

Dear Valued Customer,

We regret to inform you that there has been an issue processing your recent payment for your Netflix subscription. Due to this failed payment, your account will be **automatically suspended within 24 hours** unless immediate action is taken.

To avoid any interruption to your service and continue enjoying your favorite shows and movies, please update your payment informaton immediately by clicking the button below.

Netflix Premium Plan \$22.99/month
4 screens, Ultra HD + HDR
Account: ****@gmail.com

Payment Failed
Expires: Jan 15, 2025

Sniff & Detect

AI Insight Results Deep Scan Results

A deep scan is currently in progress...

Caution During Scan
Please avoid interacting with this email while it's being scanned. This helps keep everything safe and accurate.

Malicious 0 Suspicious 0 Clean 0 Unrated 0

Results

Domains 0 Scanning...

Email Adresse... Scanning...

IP Address 0 Scanning...

Report as Phishing

Powered by AQUILA

- The scan results are now finished and ready to check.

The image shows a screenshot of an email client interface. The email subject is "URGENT Updte Pyment Method" and the sender is a Microsoft account. The email body contains a phishing message from Netflix, stating that the user's account will be suspended due to a failed payment. The message includes a "Netfix Premium Plan" section with details like "4 screens, Ultra HD + HDR" and a price of "\$22.99/month". A "Payment Failed" warning is also present, indicating the payment expires on Jan 15, 2025.

On the right side, the "Sniff & Detect" tool interface is visible. It shows "Deep Scan Results" with a "Scan Complete" status. The overall verdict is "Unrated". Below this, there are four categories: Malicious (0), Suspicious (0), Clean (0), and Unrated (0). The "Results" section lists domains and email addresses, all marked as "unrated":

Category	Item	Status
Domains 5	netflix-billing.com	unrated
	cytechint.com	unrated
	microsOft.click	unrated
	gmail.com	unrated
	netflix-system.com	unrated
Email Adresse...	richmond@cytechint.com	unrated
	john.doe.customer@g...	unrated

A "Report as Phishing" button is located at the bottom of the tool interface. The tool is powered by AQUILA.

- This is the result of a deep scan conducted by the Sniff & Detect tool on a suspicious email impersonating Netflix.
 1. **Arrow 1** highlights the domain **netflix-billing.com**, which is flagged as a spoofed domain used to impersonate Netflix and trick users into entering sensitive information.
 2. **Arrow 2** lists phishing-related email addresses such as **richmond@cytcehint.com** and **support@netflix-billing.com**, which are likely used to send or support the fraudulent email.
 3. **Arrow 3** shows the IP address **192.168.1.45**, flagged as part of the phishing infrastructure. Although it's a private IP, its presence suggests internal spoofing or malicious setup.

The image shows a screenshot of an email client interface. The main email content is a phishing message from Netflix with the subject "URGENT Updte Pymment Method". The sender is a Microsoft Click ID. A warning message states: "Some content in this message has been blocked because the sender isn't in your Safe senders list." The email body contains the Netflix logo, the subject "URGENT: Your Netflix account will be suspended", and a message from a "Valued Customer" regarding a failed payment. A payment summary box shows "Netflix Premium Plan" for "\$22.99/month" with a "Payment Failed" warning and an expiration date of "Jan 15, 2025".

On the right side, a "Sniff & Detect" sidebar is open, showing "Deep Scan Results". It displays statistics for "AI Insight Results" and "Deep Scan Results" (all zero). The "Results" section is divided into three categories:

- Domains 5:** A list of domains with "unrated" status: netflix-billing.com, cytechint.com, microsoft.click, gmail.com, and netflix-system.com.
- Email Address...**: A list of email addresses with "unrated" status: richmond@cytechint.com, john.doe.customer@g..., billing-notifications@ne..., and support@netflix-billing...
- IP Address 1:** A list of IP addresses with "unrated" status: 192.168.1.45.

At the bottom of the sidebar, there is a "Report as Phishing" button and the text "Powered by AQUILA".

Red arrows and numbers 1, 2, and 3 point to the Netflix logo, the "URGENT: Your Netflix account will be suspended" text, and the "IP Address 1" section of the security tool, respectively.

If you need further assistance, kindly contact our support at support@cytechint.com for prompt assistance and guidance.

Revision #7

Created 8 September 2025 09:43:41 by Richmond Abella

Updated 10 March 2026 13:41:53 by Richmond Abella