Using "Account-free" Email Services to Combat Phishing, Brand Infringement, and Other Online Threats

A Review of Tactical and Regulatory Advantages

Abstract

This paper highlights the specific tactical and regulatory advantages that can be gained by tapping information and activity managed by "account-free" email service providers. An account-free email service is one that accepts all incoming email, creating email boxes for every incoming message at the time of delivery. The result is that there are no email accounts, no users or passwords, and, therefore, there can be no "expectation of privacy[1]." Due to the complete absence of user accounts, account-free email service providers are not subject to the extensive and complex privacy regulations that often constrain analysis, slow incident response, and, in some cases, shield actionable information and activity entirely. As such, the advantages of using account-free email sources include earlier detection of suspicious email, access to content that is typically unavailable to other spam/anti-phishing sources, and the ability to influence and modify email traffic to combat malicious and/or criminal campaigns.

Applicable regulations include: money laundering (such as mule recruitment), impostor customers (as required by the USA Patriot Act), and identity theft on new-customer account applications (that are required by the Red Flag regulations, which are part of the Fair and Accurate Credit Transactions Act of 2003 [FACTA]).

Author: Sebastian Holst
Advisory Board Member, Qi-fense, LLC
sebastian@qi-fense.com

---

[1] In United States constitutional law, the expectation of privacy is a legal test which is crucial in defining the scope of the applicability of the privacy protections of the Fourth Amendment to the United States Constitution. Similar concepts are expressed in the constitutions, regulations, and the courts of Canada, the EU, and other relevant jurisdictions.

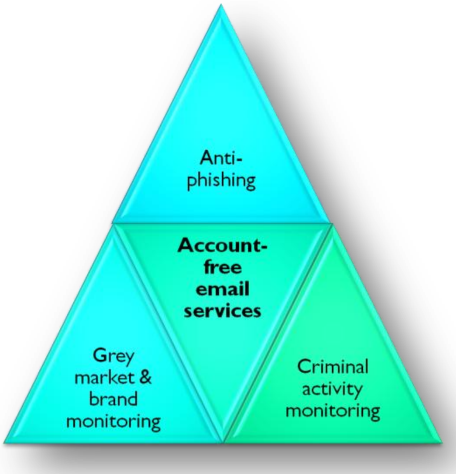

Anti-phishing
Account-free email services
Grey market & brand monitoring
Criminal activity monitoring

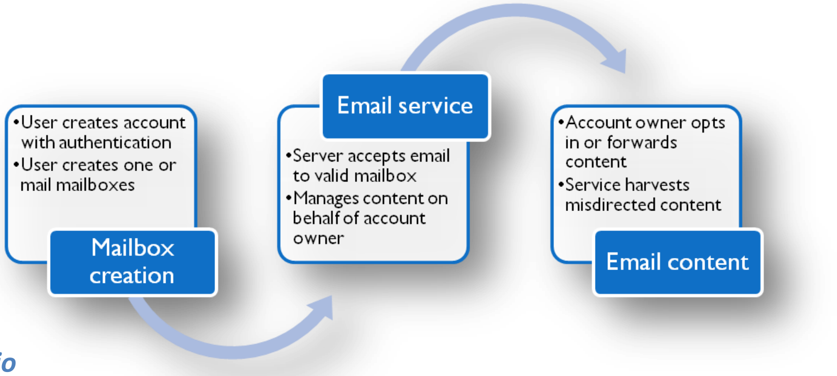
Table of Contents

Account-free Email Service

Overview

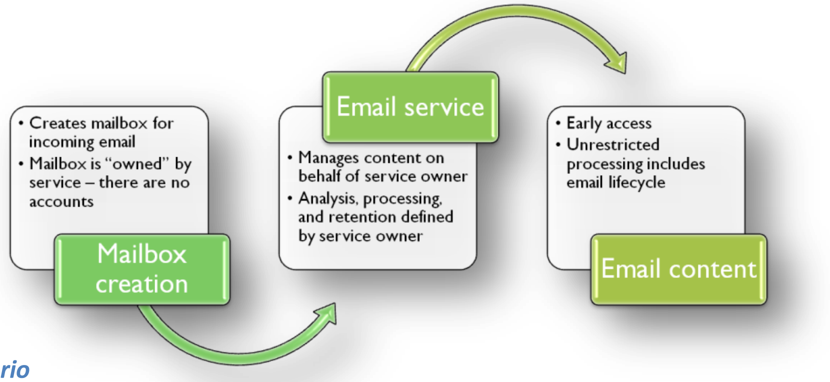
Account-free email services do not maintain a list of local or private email boxes. Rather, the account-free email server accepts email addressed to any email box.

In a typical email scenario, a user creates an account and associates one or more mailboxes with that account. The email service provider then manages the user account and mailboxes on behalf of the user. All email content and user activity is owned by the user and protected under prevailing privacy regulations[2].


•User creates account with authentication
•User creates one or mail mailboxes
Mailbox creation
Email service
•Server accepts email to valid mailbox
•Manages content on behalf of account owner
•Account owner opts in or forwards content
•Service harvests misdirected content
Email content

A Typical Email Scenario

In an account-free email scenario, the email server, *by design*, does not create accounts and mailboxes are visible to all. Mailboxes are created as email messages arrive. Email messages are publically available. Because there are no accounts and the service provider literally has no means of identifying who (if anyone) requested an incoming message, the content is owned and managed *by* the email service provider *for* the email service provider.


• Creates mailbox for incoming email
• Mailbox is "owned" by service – there are no accounts
Mailbox creation
Email service
• Manages content on behalf of service owner
• Analysis, processing, and retention defined by service owner
• Early access
• Unrestricted processing includes email lifecycle
Email content

Account-free email scenario

Account-free Email Service Use Cases

Account-free email services are used by individuals who wish to be truly anonymous. Common use cases include:

- Newsletter subscriptions
- Online account credential requests

---

[2] As a case in point, see Google's Gmail privacy policy at http://gmail.google.com/mail/help/privacy.html

Other uses include

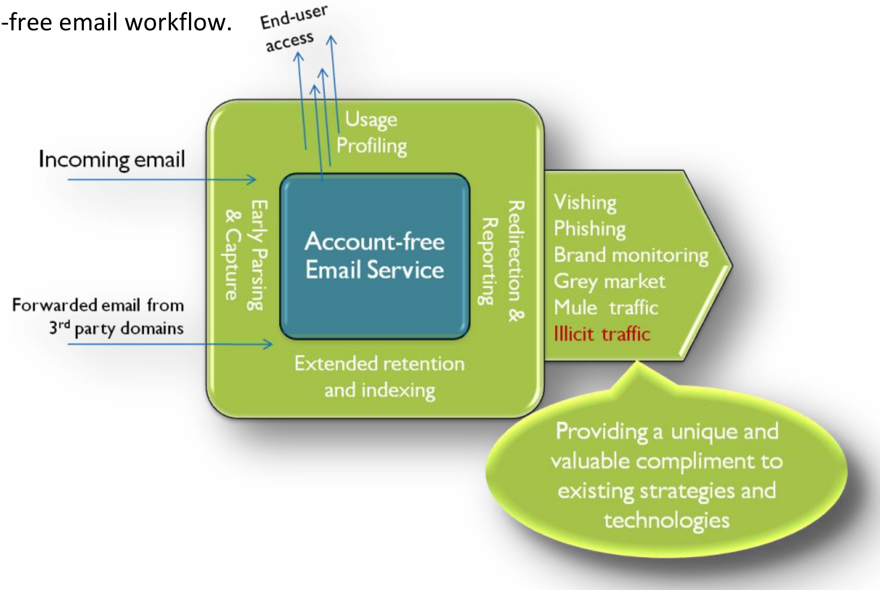
- Quality Assurance for testing applications that send email
- A forwarding destination from other domains

Another potential application, although there are no actual examples that can be cited, is as a utility within an enterprise to reduce spam targeting legitimate emails and as a means to reduce the burden of record retention obligations for non-essential email traffic.

While there is no definitive means to measure the total volume of account-free email traffic, based upon the reporting of three of the most popular account-free email sites, daily traffic varies between 5 million and 40 million email messages per day. The first recorded account-free email service debuted in July, 2003 and a second service was launched in December, 2003.[3]

Privacy Implications

Account-free email services have no users and so there is no privacy to respect. Unlike other sources of email content that must rely upon forwarded or rejected email streams, analytic software can be applied at every phase of the account-free email workflow.



End-user access
Incoming email
Forwarded email from 3rd party domains
Usage Profiling
Early Parsing & Capture
Account-free Email Service
Redirection & Reporting
Extended retention and indexing
Vishing
Phishing
Brand monitoring
Grey market
Mule traffic
Illicit traffic
Providing a unique and valuable compliment to existing strategies and technologies

Analytic opportunities within account-free email service workflows

Early parsing & data capture

Incoming email can be parsed at the instant it is being received by the email server – before it is even placed inside a mailbox. Further, there is information about the sending server, such as the IP address, that is lost once the transmission is complete. This information can be gathered and passed along with the email header, the email body, and any attachments.

Extended retention and indexing

Information can be organized and indexed across email addresses, subjects, etc. Further, referral URLs (Internet addresses embedded inside email messages) can be extracted and analyzed across all domains (sending and receiving).

---

[3] mailinator.com and dodgeit.com respectively.

Usage Profiling

In addition to email content, email functions can be monitored as well. For example, are emails opened? Are emails deleted? Are links within emails "clicked?" NOTE – this is "usage" profiling, NOT "user" profiling. There is no way to identify users of these systems.

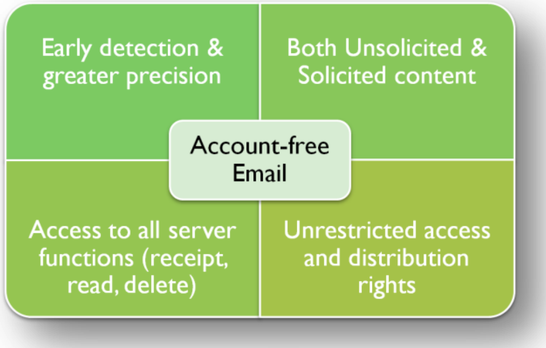
Redirection and reporting

All of the information that is gathered can be sorted, aggregated, and distributed in any form by the account-free email service provider. It is their information.

These capabilities and information sources are only possible because the email traffic, content, and usage are not (and cannot) be associated with an individual.

Tactical Advantages

Timely and targeted analysis of account-free email services can deliver the following tactical advantages over traditional sources of email content[4].


Early detection & greater precision
Both Unsolicited & Solicited content
Account-free Email
Access to all server functions (receipt, read, delete)
Unrestricted access and distribution rights

Early detection

The ability to parse and filter incoming email as it is being received enables earlier detection.

Increased transparency

The ability to guarantee sending IP addresses, have full access to header information, extract embedded URLs inside email bodies and correlate all of the above can lead to the identification of patterns and practices that are otherwise obscured.

Unsolicited and solicited communications

The stream of email traffic will include both solicited and unsolicited messages. Domain registrations, account registrations, and recruitment of "mules" are all examples of solicited email content that can be used to anticipate and defend against hostile and criminal online activities.

Email workflow monitoring

Knowing which email has been read and when can direct attention to real-time activities that trigger incident response. Activities can include spammers registering domains or suspicious account creation within social networks.

---

[4] Spam feeds, honey pots, end-user reporting, etc.

Data Mining

Archived email traffic can be used to analyze patterns and practices by industry, IP sources, phishing technique, grey market techniques, etc.

Malware analysis

Because the email content is captured prior to an email system browsing or rendering the messages, attachments and embedded images are embedded within the email stream and can be safely routed to teams equipped to do analysis and forensics on the embedded programs and rich media.

Prosecutorial tool

The ability to use disposable email archives as a discovery tool to link multiple attacks targeting different organizations by identifying common language, deceptive techniques, shared hosts and other telltale signs can enable more aggressive prosecution.

Educational Content

Email samples and the results of analysis can be used to create educational material.

Enterprise anti-spam

Account-free email software can be used within an enterprise for employees to use for newsletters, social network registrations, etc. This policy can result in lowered spam traffic and, since account-free email servers automatically purge data, retention burdens for unsolicited or non-critical email are further reduced.

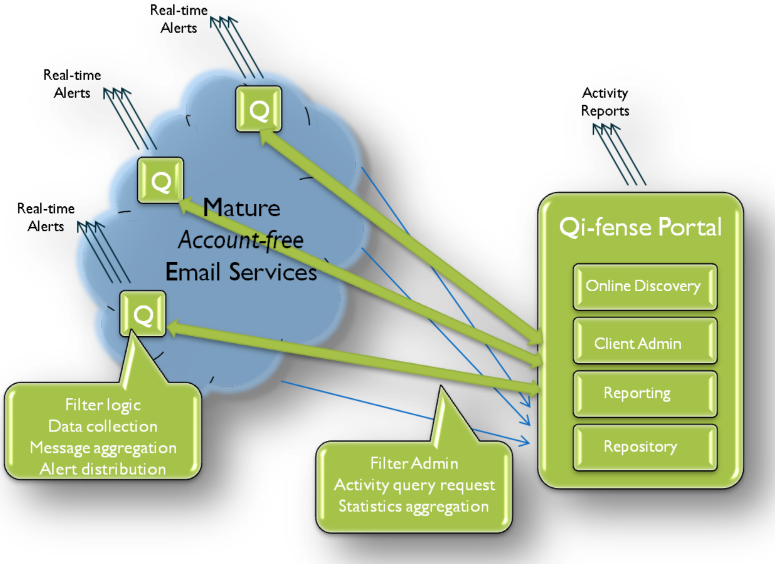
Organizational Challenges

Typically, the individuals tasked with phishing site detection, malware defense, educational outreach, and criminal prosecution are distributed across an equal number of departments. This can lead to an undervaluing of the account-free resource and a lack of coordination across these closely related activities. In order to fully exploit this resource, the capabilities and operational implications of account-free email must be recognized.

Case Study: Qi-fense, LLC

Qi-fense, LLC has secured access to a set of account-free email services and currently processes an average of 20 million emails per day (or roughly 50%-75% of all account-free email traffic).

Qi-fense Architecture



Qi-fense places software on account-free email servers that apply filters, collect critical data, aggregate multiple emails into packaged alerts, and distribute those alerts to stakeholders before the emails hit their intended email accounts.

Qi-fense administers these agents through a portal that also archives relevant traffic for trend analysis, filter testing, and reporting.

The following are specific examples of how account-free email services have improved anti-phishing defense, supported law enforcement, curtailed spammers, and secured online communities against suspected exploitation.

> "Qi-fense outperforms our existing phishing detection services and provides unique insight unavailable elsewhere."
>
> Sr. Manager | Investigations
> Retail Bank

Qi-fense filters for all occurrences of a bank inside the "from" field, inside a subject line, or embedded inside a reference URL. The result is that hundreds of emails are identified and forwarded to their investigations department for take-down.

Qi-fense filters for scams targeting US citizens. This agency added this service to an already sophisticated mix of spam feeds, honey pots, and registry searches. On average, Qi-fense was the first to identify 10% of the phishing sites.

> "Qi-fense is regularly the first to identify new phishing attacks."
> "The service has proven its value as a component of our broader anti-phishing strategy."
>
> -Special Agent,
> Federal agency

> "Qi-fense has opened up entirely new opportunities for us to explore."
>
> -Special Agent,
> US law enforcement agency

A blacklisted spamming site used an account-free email to register multiple Internet domains. Their pattern of registration created an alert that was forwarded to US authorities. With this information, it is possible to halt the attack before it could be launched while providing insight into evasive tactics that were previously unknown.