

Samples and Tools Phishing-Email

1. IRCTC Mail

Verify your number to process your refund

 IRCTC Helpdesk ([irctc-helpdesk@securesupportcloud\[.\]com](mailto:irctc-helpdesk@securesupportcloud[.]com))
to john[.]doe@mybusiness[.]com

Refund Pending



We've identified an overcharge on your recent IRCTC transactions. A refund of ₹4,240 is now pending. This link will expire in 2 business days.

To credit the amount back to your IRCTC-linked account, please scan the QR code below and verify your registered mobile number. Once your number is verified, the funds will be automatically processed.



If you cannot scan the code, use [this secure link](#).

Pending Refund

Overcharge	₹4,240
Taxes	₹0

Total Instant Refund ₹4,240


Indian Railway Catering and Tourism Corporation Ltd., B-148, 11th Floor, Statesman House, Barakhamba Road, Connaught Place, New Delhi – 110001, India.

2. ICICI Bank Mail Sample



Security Update:

Attn! Dear Customer,

We wish to inform that we are running an account upgrade of all accounts in our server database.
click on the link below to protect your account from been a victim of online hackers.
www.icicibank.com/new-security/upgrade

Important Notice:- Please match your information correctly and carefully to avoid account suspension.
Thank you for banking with us.

Accounts Management As outlined in our User Agreement, ICICI ® Bank will periodically send you information about site changes and enhancements.

Visit our Privacy Policy and User Agreement if you have any questions.

3.Microsoft Account Recover Mail

Microsoft account security alert



Microsoft 365 Support ([support@office-365-notifications\[.\]com](mailto:support@office-365-notifications[.]com))
to [john\[.\]doe@mybusiness\[.\]com](mailto:john[.]doe@mybusiness[.]com)

Microsoft account

Security alert

We think that someone else has accessed the Microsoft account [john\[.\]doe@mybusiness\[.\]com](mailto:john[.]doe@mybusiness[.]com). When this happens, we require you to verify your identity with a security challenge and then change your password the next time you sign in.

If someone else has access to your account, they have your password and might be trying to access your personal information or send junk email.

If you haven't already recovered your account, we can help you do it now.

[Recover account](#)

Learn how to [make your account more secure](#).

Thanks,
The Microsoft account team

[Privacy Statement](#)

Tools :- [This tools are tested and run icici bank mail sample]

1. virustotal

SUMO Logic URL Scan - http://www.icicibank.com/new-security/upgrade

1 / 65 security vendor flagged this URL as malicious

http://www.icicibank.com/new-security/upgrade
www.icicibank.com

Status: 200 | Content type: text/html; charset=UTF-8 | Last Analysis Date: 10 years ago

Community Score: 1 / 65

DETECTION DETAILS COMMUNITY

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Security vendors' analysis

			Do you want to automate checks?
Blueliv	Malicious	CloudStat	Clean
ADMINUSLabs	Clean	AlienVault	Clean
Anti-AVL	Clean	Avira	Clean
Baidu-International	Clean	BitDefender	Clean
C-SIRT	Clean	CLEAN MX	Clean
Comodo Site Inspector	Clean	CRDF	Clean
CyberCrime	Clean	Dr.Web	Clean

Do you want to automate checks?

SUMO Logic URL Scan - http://www.icicibank.com/new-security/upgrade

DETECTION DETAILS COMMUNITY

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Categories

BitDefender	onlinepay
Websense ThreatSeeker	financial data and services

History

First Submission	2014-09-16 07:11:51 UTC
Last Submission	2015-09-29 04:33:06 UTC
Last Analysis	2015-09-29 04:33:06 UTC

HTTP Response

Final URL: http://www.icicibank.com/sitemap.page

Serving IP Address: 63.85.36.35

Status Code: 200

Body SHA-256: 28ac2a76133de74b414e2a1817c40752a96633cad1e6aa3cc65fd602bbb97309

Analyse

2.Talos

The screenshot shows the Cisco Talos Intelligence Center interface. At the top, there's a navigation bar with links to 'Intelligence Center', 'Vulnerability Research', 'Incident Response', 'Blog', and 'Support'. On the far right of the top bar is a 'CISCO LOGIN' button and a small orange box with a warning icon labeled 'UNDER ATTACK?'. Below the navigation, a search bar contains the URL 'www.icicibank.com/new-security/upgrade'. To the right of the search bar is a magnifying glass icon. Underneath the search bar are two tabs: 'IP & Domain Reputation Overview' and 'Email & Spam Trends'. The main content area is divided into several sections:

- OWNER DETAILS**:
 - URI: icicibank.com/new-security/upgrade
 - HOSTNAME: www.icicibank.com
 - DOMAIN: icicibank.com
 - NETWORK OWNER: AKAMAI INTERNATIONAL B.V.
- REPUTATION DETAILS**:
 - WEB REPUTATION: Favorable
 - Submit Web Reputation Ticket
- BLOCK LISTS**:
 - TALOS SECURITY INTELLIGENCE BLOCK LIST
 - ADDED TO BLOCK LIST: No
- CONTENT DETAILS**:
 - CONTENT CATEGORY: Finance
 - Submit Content Categorization Ticket

At the bottom left of the content area, there's a note: 'Think these category details are incorrect?' followed by a 'Submit Content Categorization Ticket' button.

3.Browserling

The screenshot shows the homepage of Browserling, a service for online cross-browser testing and cybersecurity sandboxing. At the top, there's a navigation bar with links for Features, Pricing, Live API, About Us, Sign In, and Sign Up. Below the navigation, it says "we also created: ONLINEPINGTOOLS". The main heading is "Online cross-browser testing" and "Cybersecurity sandbox". A search bar contains the URL "www.icicibank.com/new-security/upgrade" and a "Test now!" button. Below the search bar are dropdown menus for "Windows 10" (selected), "Chrome", and "138". A large call-to-action button says "Get a browser and start testing in 5 seconds!". Below this, a section titled "Features" is shown, featuring a screenshot of a browser session. The browser window displays a 404 error page for "icicibank.com/new-security/upgrade" with the message "There's Nothing Here...". The browser interface includes a sidebar with various testing options like Operating System (Windows 10), Browser or App (Chrome 138), and URL (www.icicibank.com/new-sec). Other features listed in the sidebar include Display options, Local testing, Proxy and VPN, File transfers, Share browser, Capture screen, Show keyboard, Copy and paste, Launch apps, Send feedback, and End session.