

Sun City Computer Club

Cyber Security SIG

November 1, 2018

Is your credit card number in a hacker's database?

You can easily find out now! All you need to do is enter its information here and we will scan thousands of hacker databases to see if any they have match yours.

Credit Card Number:

Expiration Date:

Your Zip Code:



SCAN DATABASE

- Safer not Safe
- E-postcard not e-mail
- ADMINISTRATOR
- Passphrases not passwords
- Radio not wireless






Vocabulary

- Chicken Little
- Tortoise and hare
- Each of us safer, all of us safer
- Age does NOT diminish cognitive ability
- Life, Liberty, Pursuit of Happiness
- Cyber topics scare me
 - Cyber Security SIG
 - Cyber Security Blog
 - Internet

- Do nothing no problem
 <most of us>
- Do everything - catastrophic

- Neighbor's voting records via post card
- "Vote with me" app
 - all contacts, party, record, badges,
- Windows 10 zip
- Windows 10 out of band 1803 1809
- Android "regular" updates
- Apple updates everything watches
- WEB developer exploits
- **ROUTERS**
- Browsers get stronger

Current Issues

-  General
-  Home
-  Search
-  **Privacy & Security**
-  Firefox Account

Browser Privacy

Content Blocking


Block third-party content, like ads or code, that can slow your browsing and track you around the web. Customize your settings for the best balance of protection and performance.

[Restore Defaults](#)

[Exceptions...](#)

[Learn more](#)

Choose what to block

 **All Detected Trackers**
Block all known trackers. (May prevent some pages from loading.)

Only in private windows

Always

[Change block list](#)

 **Third-Party Cookies**
Block all third-party cookies or just those set by trackers.

Trackers (recommended)

All third-party cookies (may cause websites to break)

Send websites a "Do Not Track" signal that you don't want to be tracked [Learn more](#)

Always

Only when Firefox is set to block Detected Trackers

- Multiple
- Don't abandon/delete
keep active, but unused
- Email client vs. email WEB
WEB settings – download & delete
- Email in the clear
tcp connection/handshake
tcp sequence number
packet size

Email (e-postcard)

- Header envelope

Email (ePostcard)



Netflix - Thank you! <support@dealsflip.com>



[Unsubscribe](#) | [Report Spam](#)



[Unsubscribe Here](#)

2380 Corporate Circle Henderson, NV 89074

🔒 <https://webmail.suddenlink.net/do/mail/message/viewDetail?msgId=INBOXDELIM1014>

Date: Wednesday, October 31, 2018 6:34 AM

From: info@suddenlink.net

To: [REDACTED]

Cc: [REDACTED]

Subject: Your Suddenlink Bill is Now Available

Size: 9 KB

Full message



[View Entire Message](#)

document

Content-Type: text/html; charset=us-ascii

Content-Disposition:

[Open Attachment](#)

[Close](#)

suddenlink

Delete



Spam



Mark as read



Shift+K

Mark as unread

K

Star

L

Clear star



Shift+L

Block Senders

View raw message

yahoo

← Reply

➡ Forward

Filter messages like this

Print

Add New Today on Komando.com to Contacts list

Delete this message

Block "New Today on Komando.com"

Report spam

Report phishing


Show original

Translate message

Mark as unread



gmail

- Reply
- Reply all
- Forward
- Delete
- Mark as unread
- Flag
- Add to Safe senders
- Mark as junk
- Mark as phishing
- Block Balance Rewards
- Create rule
- Print
- Show in immersive reader
- View message source**
- Open in new window
-  Get Add-ins

outlook

X-Apparently-To: [REDACTED] Oct 2018 13:56:20 +0000
Return-Path: <support@dealsflip.com>
Received-SPF: pass (domain of dealsflip.com designates 5.226.175.78 as permitted sender)
X-VMailID: Y5IBtrAAdDri587vkD5Jy9ZDX25QDJkVzWRkXebectQ1zIQ_5r
5VnMLZ0H3lncwKtpdgn2nrRdWkPI6NPt5.61_V_5D51nkD1rF87bA5wy7K
VfkyrcHgdHbGp412kCBp_1jNq1fCcIP8K9VhHk6s0rRQ0b1GufadLrqFYP
ZNA9S50NhdndDAFO14X775YxtJ3VpSnoxMM4L8QdG4a527v_TK106KzFqOhh
wYD6KdG5ILF6D1_cbfwM45Kqkxq1dF4S8k88PbDctQLJQkYKDEIU3QwQ
Yj_Uj3K2NbsvEuYuHJQ87Ely4pa93dhFpVkyYjFujweh3qchTnJ8V2hdvVL
yqrdI3.nvALPjL1sT5CbcbFVbEhfWq0icw0H1IQ82TNSLpE3xrLXdW2K1YV
R3_d0HQ1RoMby1Vr9IU_X8Se8bu1rH8Juqnt9u0wG2NiE3F8Q9V81GEmWxX
foIySezLq3d3NGSRTgjj7QRRaIxyWV8E0a1q50GntA117E34PKXBe5QeMy
X8OCQDSEPaehajkgLTYdjtTRV8Bt1904191a.CQoa8d5PPM_G1EN8MAU5J
SHQ525eat8UDNSajQeF9gSu_1FEarmip2HfSqLD17URtk0P1EPeQMeNpmtQ
rIvuXccIgJa55j41N46s9ZdM42cP8jrT1fH9FLWuCorFTQAJCj66IU2q.P
Kz0HQY4ERv90-OrbIV1_kTP2R3iw2MtLuNpaX40uYR9vkT9I7Z3KL6eUQN_
9gEkW7ikAR1pa80IzGYE_vkRI.n8qgpJ79g_tAmfSw0sAlGF768KRvYxyc_6
htHwzufPzrcrCasCeznKckdNAlryBEUCyFuRD_0Ufee76SwoFDGRPV8M1X
77zoM1d.tbfgtq3ZeTrwUc3p2062FGrouTentrXGno211_.5h58P0T.mubI
IYeQ0Lb3eRZ3wo4KBU2eqIuo0gWnCayuve.qkw_sorVGRB0TP8eoyTagEha
gIrPAiNKGsqVfQkMktIuQ_g8sPjghSooRYVcL.Adn8uy8hCME5V9T2R-Exgp
Geeoh_r1MgKjbaA5QaNJVKYxc6jJVRwqEylJ2B2xyeGdLcR9a6rKqPHzsk
H7QnAfdRe15RHGg034h8vG84ofixtUNE88BtW9AA5yNAUTbPDGgJkh
jTEo7ZvT03uDX1Y5USFQR_CAFnRo1RonvIF5fc-
X-Originating-IP: [5.226.175.78]
Authentication-Results: sta4259.mail.nel.yahoo.com from=dealsflip.com; domainkeys=neutral (no sig); from=dealsflip.com; dkim=pass (ok)
Received: from 127.0.0.1 (EHLO dlfp-175078.dealsflip.com) (5.226.175.78)
by sta4259.mail.nel.yahoo.com with SMTP; Wed, 31 Oct 2018 13:56:19 +0000
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed; d=dealsflip.com;
q=dns/txt; s=dk2048; bh=szajlM4le+q0E5nxIgwVW123UJaaITCRK+7Ks8r3lCV+;
h=from:reply-to:subject:to:mime-version:content-type:content-transfer-encoding:list-unsubscribe;
b=X1xL/3Wu8M0DNf4XDCp1f10Xvbhd9VbVf/HURTo2x9WdVx5BPK25vTynmlyIQ5N1euV5
nZD6sJGvrIzc6wDURgZtr/rfQv/sQqvKq4aopFzYLMmGyCBAkRvgthmUet-wkZgp1ThZv+q8F0
ft0t4z3Z/90Z0WwSGBKH8D5ZD+1e6GqFmRqGD+17BltnW/2wtf3E7xwVLaXsD5OY12RntDi4E
b1d65vY/8Ztvb2V6S8ZkncP3lwQeG1c2LAHYEV2uz0R/gqTDrjs2XGNWfY180bkh1LFs06F6J
35s+H8rgenQ70RrQVhCugz94Mepqhg7L1uaQqHPKpFyw==
Content-Type: text/html; charset=UTF-8
From: =?UTF-8?B?1xv02xpeCAT1FRoVw5rIhVdSE=?> <support@dealsflip.com>
To: [REDACTED]
Reply-To: support@dealsflip.com
Subject: =?UTF-8?B?Q29uZ1JhdVxyYXRpb24gam90biBqZm5wZm5zb24h?=>
Message-ID: <null_106743024_9399432_9266549_951708_281_910_4940.1548994414436.com.root@d1fp-175078.dealsflip.com>
X-Mailer: <support@dealsflip.com>
X-Complaints-To: <abuse@dealsflip.com>
List-Unsubscribe: http://t.dealsflip.com/p/?j1=2HdyFOIw2GTyFHWAc62HEYECh7ENTUEclMFCETE0h=8-j2=2c16316E6Uy1jpvKVVOKyw62HATDchYfC86E00u
Content-Transfer-Encoding: quoted-printable
Date: Wed, 31 Oct 2018 13:56:19 GMT
MIME-Version: 1.0
Content-Length: 1985

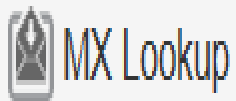
<meta http-equiv=3D'Content-Type' content=3D'text/html; charset=3DUTF-8'><<enter>=0A <head></head>=0A =0A <table style=3D'max-width:600px; table-layout:fixed; margin:0px auto;padding-top:10px;padding-bottom:10px;" width=3D"100%" cellpadding=3D"0" cellspacing=3D"0" border=3D"0" align=3D"center">=0A =0A <tr>=0A <td align=3D"center">Unsubscribe =0A </td>=0A </tr>=0A <tr>=0A <td align=3D"center">Report Spam</td>=0A </tr>=0A </table>=0A =0A <table width=3D"100%" border=3D"0" cellpadding=3D"0" cellspacing=3D"0" align=3D"center" style=3D"max-width:600px;padding-top:15px;table-layout:fixed;margin:0px auto;">=0A <tr>=0A <td align=3D"center"></td>=0A </tr>=0A <tr>=0A <td align=3D"center" style=3D"font-family:Arial, Helvetica, sans-serif;font-size:11px;padding-top:10px;line-height:17px;"> Unsubscribe Here
 2360 Corporate Circle Henderson, NV 89074 </td>=0A </tr>=0A </table>=0A </center>



https://mxtoolbox.com/



- [MX Lookup](#)
- [Blacklists](#)
- [Diagnostics](#)
- [Domain Health](#)
- [Analyze Headers](#)
- [Free Monitoring](#)
- [DMARC](#)
- [Investigator](#)
- [DNS Lookup](#)
- [More ▾](#)



Domain Name

MX Lookup

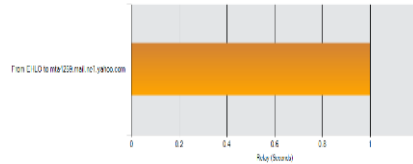
Solve Email Delivery Problems

Header Analyzed

Email Subject: =?UTF-8?B?Q29uZ3JhdHVsYXRob24gamlob2ZlW5raW5zd247=?

Relay Information

Received Delay: 0 seconds



Hop	Delay	From	By	With	Time (UTC)	Blacklist
1	*	EHLO 127.0.0.1	mta4259.mail.net1.yahoo.com	SMTP	10/31/2018 1:58:19 PM	

Are people getting your messages? Find out with Mx Delivery Center!

- Daily Updates on Delivery issues including Microsoft and Gmail.
- Support to setup your DMARC, DKIM, and SPF Records!

[Learn More](#)

Headers Found

Header Name	Header Value
X-Apparently-To	jenkinsrjp@yahoo.com; Wed, 31 Oct 2018 13:58:20 +0000
Return-Path	<support@dealstip.com>
Received-SPF	pass (domain of dealstip.com designates 5.228.175.78 as permitted sender)
X-YMailSG	YSBhAWLQusS87MOSjAZQSD0.KZVRrXehedQ2Q_5r 5VhMLZ0UlmowKp4gn2prRaDwXp8NP5.B_Y_5D6NiDhF87a5wyr7K_VkyrcWgM8bGp2mC8g_1pQ1FocZpK0vhrK0v8Dr00dGSubadLqFYP_ZNA9sOhHdmDAM0A7YYUJ3p5rWw4HL00dG4e527v_#006WzqOhh_wY0GqSILF6D_cbrfwN49qW0xq1dY4S880Ph6cTQLJQYKDEIU0wQ_YJUGKZkbnGvUvHU007Ely4ps83dhFxmMYf4jwv3qzphTNBv2hdV_V_ygrd3.mALPjT5tCb_dwYmFMwq01cwmfH#QBZNSLpLpLxLxW2R1Yv_R3_d0Q1RoM8yY199U.XbbeBw3h8Ljqr8u8w82NEsF809/B1GEWwX_fay8ezLp3d3NGSRTgg7QPR8xYVW06Dn1sG0hA1H1EJ4PKX8e50eMy_X80000DSEPehahkg_TjQjTRV8m18D419a.CQwb8jSPW1_GEr8MAU5j_SHQ52se8tBUDN5qQeF8bu_1FEampZIF8q.D7UKtoOPEPOMeNpmD_rlvKcdJss54N46sZzWwM4z2mP8jT1H8FUw_CorFTDAJQ6hUQz_P_KchD2Y4ER/gW1Dh61_ATP2R_JwG2MuNpa4QUYRHkT917z3K6uLQON_8qEwTKAR1a8bduGYE_WRLnBqppJ79g_UmF8uJcAjF780kRvYyqz_8HhWzuffzrzcAaCzcmKkdN1fryeUJyARU_DJf0e705wOFGEpVbWYX77zoM1bf9g3ZmTck3p0z7GruuTerinGnc2L_8i68POT.mUl_Y6CbLkRZ3W4K8L2equb0gW0rCaywe.qWw_soRVGRB0TP8oyTagEVA_gPAINq6qVOKM3uQ_g8Pgh50atMYvLd_ACh6y8rCMsV98Z78yq_Gebch_rIMGkA650ANVYx6jJWwEJL2B2s_yeGmC8R8ubqkP1zzsk_H7qtoA68re15RkGqD348vG84oFxdLINEm888w8w0A5yN8UJtPODgJhJTEnZ7T03uXYSU8IQR_CAhRo1Ranvml5lc
X-Originating-IP	[5.228.175.78]
Authentication-Results	mta4259.mail.net1.yahoo.com from=dealstip.com; domainkeys=neutral (no sig); from=dealstip.com; dkim=pass (ok)
DKIM-Signature	v=1; a=rsa-sha256; c=relaxed/relaxed; d=dealstip.com; q=dns/dkim; s=ok2048; bh=3smJMIe+eE05m8gNWY23Uaal.T8R9-7k5d3k1c;-; h=from:reply-to:subject:mime-version:content-type:content-transfer-encoding:is-unsolicited; b=X1eE38w8W00N4X0p1H10Wbwh9VhrHURThZz68W0X58Mw25Vjrmjy30SN1euV5_nZD6gGrLcC8wDURqZRHf4VwQ0Kq4axpZ2YLMmGyCJW8RvgImUmt+wKkgpThZ+wq8oR04kZ90Z0wSG8W805ZD+h8GqJfFR_gSD+17B8N2W8E7xwVLaXkD50Y2RNDIE4y_b1s85y18ZvUv8S0zencP3wQvGkZLhY1EYzucORjgD2XGNWfY808hLFL5d8FG3m_35e+H0geq7OR0W1LJg94MepqG7L_uwDqjFPkGfFw=
Content-Type	text/html; charset=UTF-8
From	=?UTF-8?B?Q29uZ3JhdHVsYXRob24gamlob2ZlW5raW5zd247=? <support@dealstip.com>
To	jenkinsrjp@yahoo.com
Reply-To	support@dealstip.com
Subject	=?UTF-8?B?Q29uZ3JhdHVsYXRob24gamlob2ZlW5raW5zd247=?
Message-ID	<ul_106743024_9360432_9266549_951708_281_910_4940_1540984414436.com.root@dlp-175078.dealstip.com>
X-Mailer	<support@dealstip.com>
X-Complaints-To	<abuse@dealstip.com>
List-Unsubscribe	http://dealstip.com/p/1-21hYF0w2GTYfHWec02HEYEch7ENTUEDWfETEDH=4-q2=2a83L8E3UjYpW4YOKy62H4TDCdYf08E0du
Content-Transfer-Encoding	quoted-printable
Date	Wed, 31 Oct 2018 13:58:19 GMT
MIME-Version	1.0
Content-Length	1988

Website: dealsflip.com

Website screenshot showing a promotional banner for Tata Cliq Anniversary Sale with 80% Off - Extra 10% Off On Electronics, Mobiles, Laptops, Fashion Products. The page includes a search bar, a navigation menu, and a list of recent products.

Url: dealsflip.com

Related Domains

Upgrade to get more information. [Learn more](#)

Domain	IpAddress	GoogleAdsenseld	ScannedOn
dealsflip.com	51.255.68.119		2016-12-15T21:52:04.192Z
***nextgen.com	51.255.68.119		
***9zip.com	51.255.68.119		
***nplacemail.com	51.255.68.119		
***livemessage.com	51.255.68.119		
***rs.com	51.255.68.119		
***giz.com	51.255.68.119		
***persvid.com	51.255.68.119		

Related IPs

Upgrade to get more information like Reverse DNS, Geo Location, ASN and CIDR block. [Learn more](#)

Ip	Reverse DNS	Location	ASN	CIDR
51.255.68.***	ns3029097.ip-51-255-68.eu	FR 🇫🇷	16276 (OVH SAS)	51.254.0.0/15
205.251.194.***	ns-738.awsdns-28.net	Seattle, WA US 🇺🇸	16509 (Amazon.com, Inc.)	205.251.192.0/21
205.251.198.***	ns-1604.awsdns-08.co.uk	Seattle, WA US 🇺🇸	16509 (Amazon.com, Inc.)	205.251.192.0/21
205.251.193.***	ns-415.awsdns-51.com	Seattle, WA US 🇺🇸	16509 (Amazon.com, Inc.)	205.251.192.0/23
205.251.197.***	ns-1361.awsdns-42.org	Seattle, WA US 🇺🇸	16509 (Amazon.com, Inc.)	205.251.192.0/21

This product includes GeoLite data created by MaxMind, available from <https://www.maxmind.com>.

Name Servers

Upgrade to get more information. [Learn more](#)

Domain Name	IP Address	TTL
*****1.awsdns-42.org	205.251.***.***	48 hrs
*****4.awsdns-08.co.uk	205.251.***.***	48 hrs
*****awsdns-51.com	205.251.***.***	48 hrs
*****awsdns-28.net	205.251.***.***	48 hrs

MX (Mail Exchanger Record)

Upgrade to get more information. [Learn more](#)

Pref	Hostname	IP Address	TTL
10	*****dealsflip.com	5.226.***.***	60 min

SPF (Sender Policy Framework)

Upgrade to get more information. [Learn more](#)

Prefix	Type	Value	PrefixDesc	Description
record	*****	*****f1 a****spf1****il		
v	version	*****		The SPF record version
+	a	*****	Pass	Match if IP has a DNS 'A' record in given domain
+	mx	*****	Pass	****h i**** th**** dom****
+	include	*****	Pass	The specified domain is searched for an 'allow'.
~	all	*****	SoftFail	****ys m****oes ****ecord.

DMARC (Domain-based Message Authentication, Reporting and Conformation)

Upgrade to get more information. [Learn more](#)

Tag	TagValue	Name	Description
*****	record	*****ARC1****100,****r@de****	
v	*****	Version	****ti****d re****ecor****in ****
p	*****	Policy	****cy ****mail****C le****qua****
pct	*****	Percentage	****perc****ells****pply****ails****e.
rua	*****	Receivers	**** of ****eive****ack ****addr****amp****

Blacklists

Upgrade to get more information. [Learn more](#)

Name	Response Time
BSB Domain	141
ivmURI	141
SEM FRESH	125

Whols

Upgrade to get more information. [Learn more](#)

Investigator

Security threats are everywhere. Have the right tool to make your analysis easier

Comprehensive information on a domain in a single-pane view
Nameserver, DNS records, Whois, Blacklist, related site info and more...

[Learn more](#)

- Kim Komando - ADs
- twit.tv
- isc.sans.org
- YouTube
- Sun City Computer Club

Resources

- Tortoise and Hare
- Chicken Little

Computer Club, Help Center, SIGs,
Presentations

Cyber Security SIG meetings, NEWSBLOG
Internet

- Questions, suggestions, comments?

SCCCCyber@gmail.com