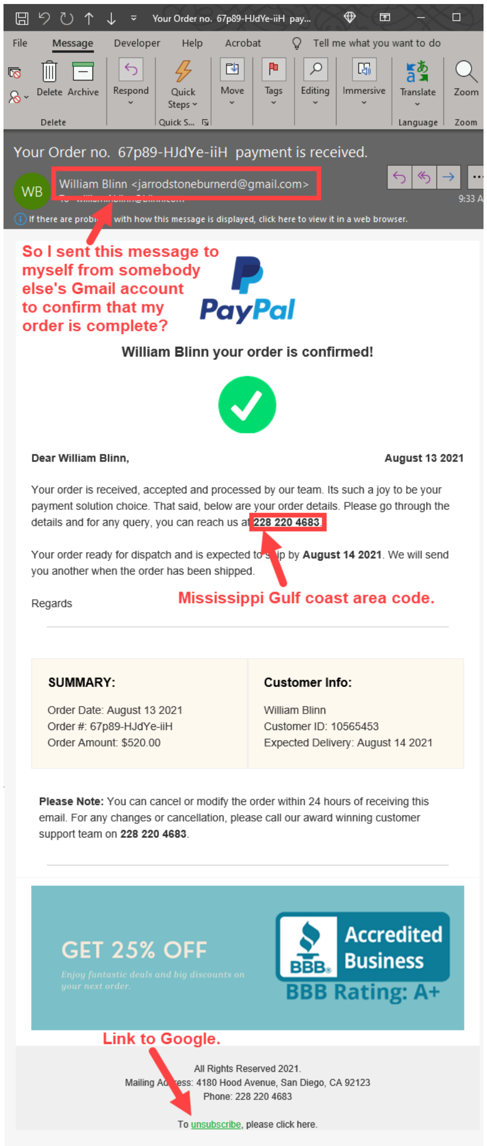
BLINN.COMmunications
September 2021
179 Caren Avenue • Worthington • Ohio 43085-2520 • 718.577.1054 (NYC) • 614.785.9359 (Ohio)

Fighting Back Against Spam and Scams with Software

INTERNET SPAM AND SCAMS BECOME WORSE EVERY YEAR. SECURITY DEPENDS ON CRITICAL THINKING, BUT AUTOMATED PROCESSES CAN HELP.



Your Order no. 67p89-HJdYe-iiH payment is received.

William Blinn <jarrodstoneburnerd@gmail.com>

If there are probl… with how this message is displayed, click here to view it in a web browser.

So I sent this message to myself from somebody else's Gmail account to confirm that my order is complete?

William Blinn your order is confirmed!

Dear William Blinn, **August 13 2021**

Your order is received, accepted and processed by our team. Its such a joy to be your payment solution choice. That said, below are your order details. Please go through the details and for any query, you can reach us at **228 220 4683**.

Your order ready for dispatch and is expected to ship by **August 14 2021**. We will send you another when the order has been shipped.

Regards

Mississippi Gulf coast area code.

SUMMARY:	Customer Info:
Order Date: August 13 2021 Order #: 67p89-HJdYe-iiH Order Amount: $520.00	William Blinn Customer ID: 10565453 Expected Delivery: August 14 2021

Please Note: You can cancel or modify the order within 24 hours of receiving this email. For any changes or cancellation, please call our award winning customer support team on **228 220 4683**.

Link to Google.

All Rights Reserved 2021.
Mailing Address: 4180 Hood Avenue, San Diego, CA 92123
Phone: 228 220 4683

To unsubscribe, please click here.

Thinking before acting is essential. Consider a message "from" PayPal. It's clearly a scam, so let's examine the obvious clues:

Although the message claims to be a PayPal message, my name is shown as the sender and the displayed address is somebody else's Gmail account. There's no need to look further, but much remains to be found.

- Merchants, not PayPal, send purchase confirmations.
- The message says that the unidentified $520 purchase will be delivered tomorrow, but that I can cancel the order within 24 hours. (Huh?)
- An unsubscribe link at the bottom of the message goes to Google.
- The phone number offered to cancel the order goes to a number in Mississippi.
- The text was written by someone with a minimal understanding of English
- An advertisement is combined with a phony Better Business Bureau graphic.

So the person who created this scam is an idiot, but many scammers are intelligent, and even this scam displays a bit of advanced thinking. Except for the unsubscribe link, there's nothing click. Those who are sufficiently well informed to know that email links can be hazardous might not attach the same concerns to the phone number.

PayPal would provide a toll-free number, and any standard number would be in a San Jose area code, where PayPal's primary office is, but the San Diego street address shown on the email doesn't exist.

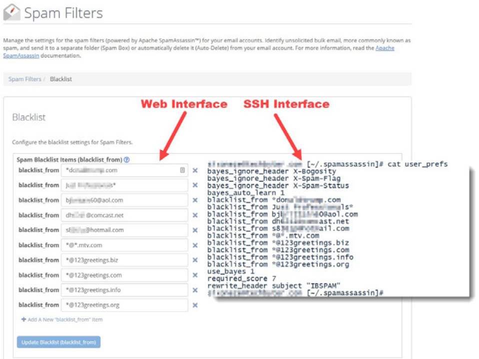
What happens if you call the phone number? You'll probably be told that someone has used your credit card to place an order. To cancel it, they will need your credit card number, your name as it appears on the card, your billing postal code, and the card's security number to cancel the order. Give them that and, although your credit card hasn't been used by crooks yet, it soon will be.

Cutting Spam Limits Scams

SEVERAL METHODS EXIST FOR DEALING WITH SPAM, EITHER ON THE SERVER OR ON YOUR COMPUTER. LET'S CONSIDER ONE SERVER-BASED OPTION FIRST.

Those who receive mail through their own domain (such as blinn.com) and have access either to the server's control panel or secure shell can activate one of the internet service provider's anti-spam functions.

SpamAssassin, installed by many ISPs, analyzes messages, scores them, and marks them as possible spam so that they can easily be identified when an email application downloads them.


Spam Filters
Spam Filters / Blacklist
Add A New "blacklist_from" Item
Update Blacklist (blacklist_from)

Manage the settings for the spam filters (powered by Apache SpamAssassin™) for your email accounts. Identify unsolicited bulk email, more commonly known as spam, and send it to a separate folder (Spam Box) or automatically delete it (Auto-Delete) from your email account. For more information, read the Apache SpamAssassin documentation.

Web Interface SSH Interface

Blacklist

Configure the blacklist settings for Spam Filters.

Spam Blacklist Items (blacklist_from)

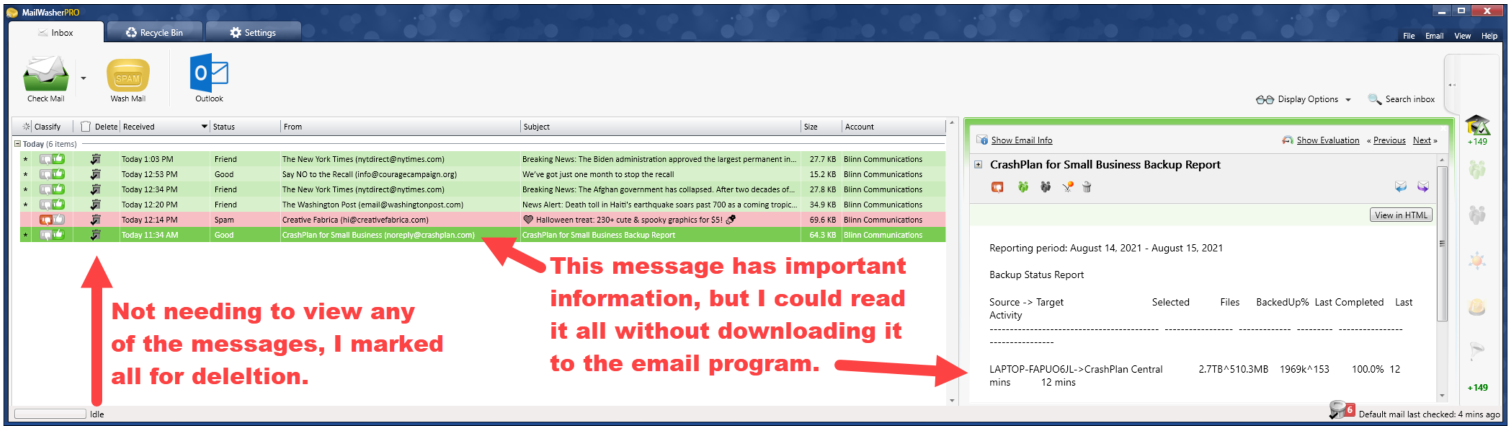
blacklist_from	*do[redacted].com
blacklist_from	Ju[redacted]*
blacklist_from	bj[redacted]60@aol.com
blacklist_from	dh[redacted]@comcast.net
blacklist_from	s[redacted]@hotmail.com
blacklist_from	*@*.mtv.com
blacklist_from	*@123greetings.biz
blacklist_from	*@123greetings.com
blacklist_from	*@123greetings.info
blacklist_from	*@123greetings.org

```
[redacted] [~/.spamassassin]# cat user_prefs
bayes_ignore_header X-Bogosity
bayes_ignore_header X-Spam-Flag
bayes_ignore_header X-Spam-Status
bayes_auto_learn 1
blacklist_from *do[redacted].com
blacklist_from Ju[redacted]ls*
blacklist_from bj[redacted]0@aol.com
blacklist_from dh[redacted]ast.net
blacklist_from s8[redacted]ail.com
blacklist_from *@*.mtv.com
blacklist_from *@123greetings.biz
blacklist_from *@123greetings.com
blacklist_from *@123greetings.info
blacklist_from *@123greetings.org
use_bayes 1
required_score 7
rewrite_header subject "IBSPAM"
[redacted] [~/.spamassassin]#
```

The server application has blacklist and whitelist sections. A whitelisted address will never be marked as spam; a blacklisted address will always be marked as spam.

Even though I have full access to the server and could easily set up SpamAssassin, I prefer to use MailWasher Pro on my computer. I've used it for nearly a decade because it gives me a way to delete spam before my email applica-

Blinn Communications News (ISSN 2639-5762) is for clients and friends of William Blinn Communications, Worthington, Ohio.
Phone 614.785.9359 (Columbus) and 718.577.1054 (NYC). On the Web at www.blinn.com. All rights reserved.



Classify	Delete	Received	Status	From	Subject	Size	Account
Today (6 items)							
*		Today 1:03 PM	Friend	The New York Times (nytdirect@nytimes.com)	Breaking News: The Biden administration approved the largest permanent in...	27.7 KB	Blinn Communications
*		Today 12:53 PM	Good	Say NO to the Recall (info@couragecampaign.org)	We've got just one month to stop the recall	15.2 KB	Blinn Communications
*		Today 12:34 PM	Friend	The New York Times (nytdirect@nytimes.com)	Breaking News: The Afghan government has collapsed. After two decades of...	27.8 KB	Blinn Communications
*		Today 12:20 PM	Friend	The Washington Post (email@washingtonpost.com)	News Alert: Death toll in Haiti's earthquake soars past 700 as a coming tropic...	34.9 KB	Blinn Communications
		Today 12:14 PM	Spam	Creative Fabrica (hi@creativefabrica.com)	♥ Halloween treat: 230+ cute & spooky graphics for $5!	69.6 KB	Blinn Communications
*		Today 11:34 AM	Good	CrashPlan for Small Business (noreply@crashplan.com)	CrashPlan for Small Business Backup Report	64.3 KB	Blinn Communications

CrashPlan for Small Business Backup Report

```
Reporting period: August 14, 2021 - August 15, 2021

Backup Status Report

Source -> Target                    Selected      Files     BackedUp%  Last Completed   Last
Activity
--------------------------------------- ---------------- ------------ --------- ---------------
----------------

LAPTOP-FAPUO6JL->CrashPlan Central        2.7TB^510.3MB   1969k^153      100.0%  12
mins         12 mins
```

Default mail last checked: 4 mins ago

Not needing to view any of the messages, I marked all for deleltion.

This message has important information, but I could read it all without downloading it to the email program.

MailWasher Pro's inbox view shows all messages that are on the server and have not yet been either downloaded to the email application or moved to the application's Recycle Bin. Any message in the recycle bin can be recovered if the user accidientally deletes a needed message.

tion downloads it. A free version can monitor only a single mail account and does not contain a Bayesian learning component. The Pro version can monitor multiple accounts, enables a learning feature, and offers additional capabilities and support.

I like this approach because I can quickly review a list of all messages on the server and decide whether to let the email application retrieve them.

I subscribe to several newspapers and news organizations that send email updates. I've whitelisted their domains, but I rarely need to read the email updates and I can delete them from the server.

I receive daily messages from a backup program. Successful backup messages always contain "if blank, no errors" in the subject; if there are no errors, I don't need to download the messages.

MailWasher Pro marks messages for deletion from any sender or domain that I've blacklisted, from dodgy sites known to blacklisting organizations, and whenever its analysis indicates the message is probably a spam. I make the final decision, quickly reviewing the list of messages on the server so that the email application will download just the few messages I want to see.

Beware Questionable Domains

I have set up MailWasher Pro to mark as spam any messages from certain top-level domains.

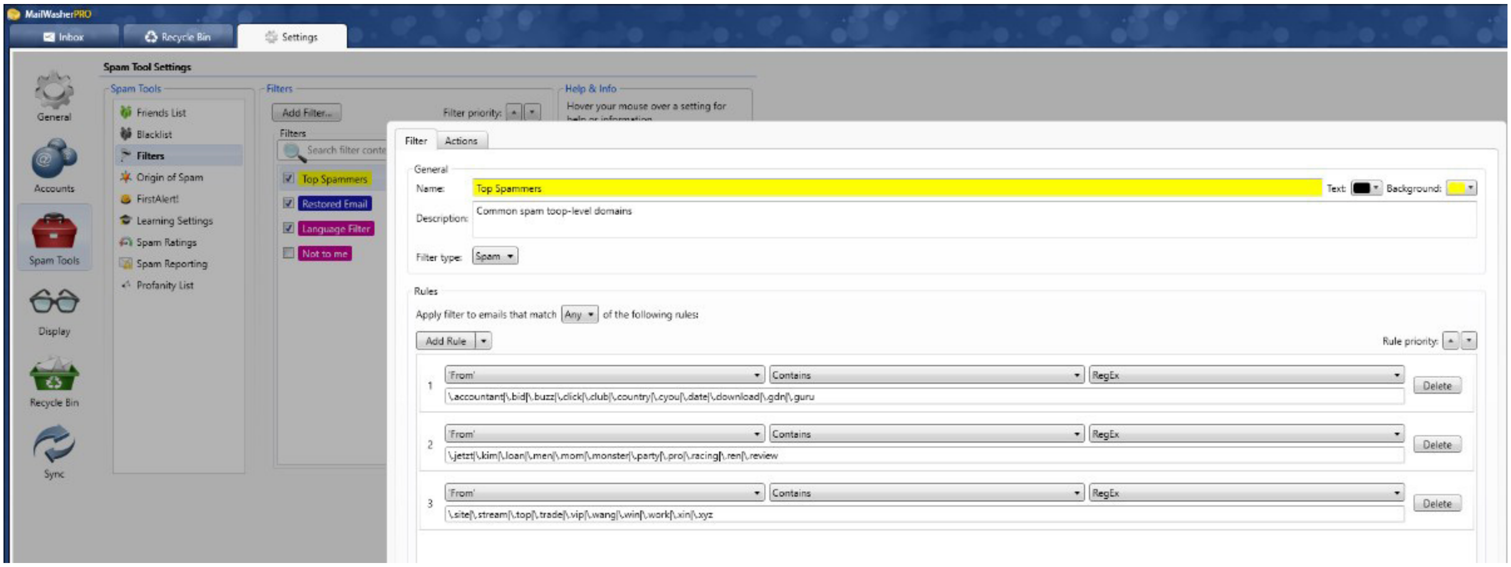
Many new top-level domains have joined .com, .org, .gov, and .edu in recent years. These TLDs aren't inherently less trustworthy than the older ones, but scammers seem to like them and I have never received a valid message from any .accountant, .bid, .buzz, .click, .club, .country, .cyou, .date, .download, .gdn, .guru, .jetzt, .icu, .kim, .loan, .men, .mom, .monster, .party, .pro, .racing, .ren, .review, .site, .stream, .top, .trade, .vip, .wang, .win, .work, .xin, or .xyz address.

MailWasher Pro users can scan through message on the server and decide which ones to delete, and accidentally deleting a message isn't a problem because the application retains messages for a while. The user decides how long "a while" is, and messages in the Recycle Bin can easily be restored.

Like SpamAssassin on servers, MailWasher Pro offers whitelists (messages will be considered good regardless of content) and blacklists (messages will always be considered spam).

Although automation, either on the server or on your local computer, can help reduce spam and alert us to scams, we humans must be the final line of defense.

MailWasher Pro users can define filters using regular expressions or, for those who don't want to master the basics of regular expressions, plain-text.



General

Name: Top Spammers Text: ■ Background: 🟨

Description: Common spam toop-level domains

Filter type: Spam

Rules

Apply filter to emails that match Any of the following rules:

1 'From' Contains RegEx
`\.accountant|\.bid|\.buzz|\.click|\.club|\.country|\.cyou|\.date|\.download|\.gdn|\.guru`

2 'From' Contains RegEx
`\.jetzt|\.kim|\.loan|\.men|\.mom|\.monster|\.party|\.pro|\.racing|\.ren|\.review`

3 'From' Contains RegEx
`\.site|\.stream|\.top|\.trade|\.vip|\.wang|\.win|\.work|\.xin|\.xyz`