

Exhibit 2023

[Blog](#)[Tips and Tricks](#)[Starter Kit](#)[Inspiration](#)[Specials](#)[Tutorials](#)[Home](#) / [Blog](#) / [Tips and Tricks](#) / [Most Common Spam Emails You Can Encounter in 2024](#)

Tips and Tricks

Most Common Spam Emails You Can Encounter in 2024



In this article

Why am I getting spam emails?

Most popular phishing and spam examples of 2024

How to identify a junk message quickly

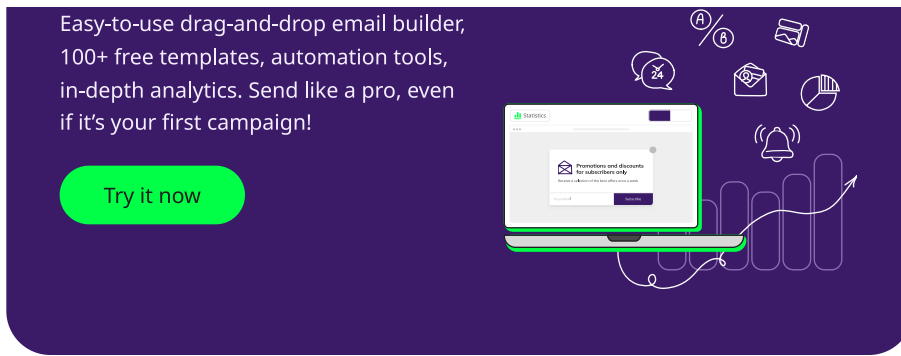
Wrapping up

Share:



In this article, we'll talk about junk mail and list the most common spam email examples. We'll provide answers as to why you receive junk mail in the first place, how to recognize it, and what are the most common spam emails.

[Try Selzy for free](#)



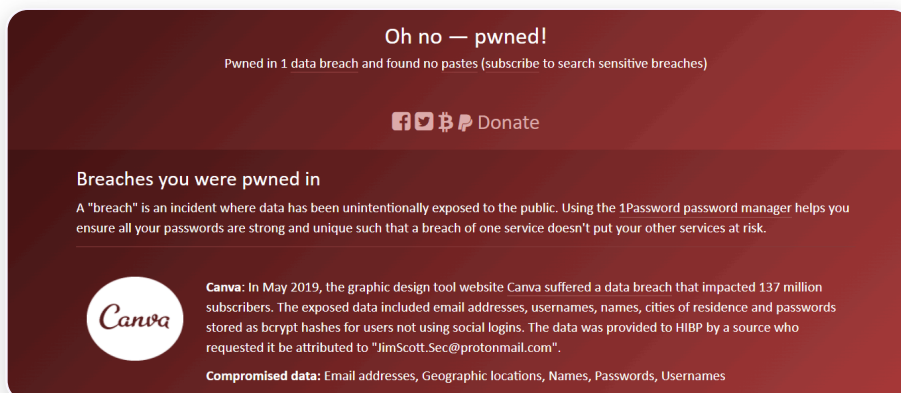
Why am I getting spam emails?

Let's take a look at some common methods that spammers use to obtain email addresses — and how to protect yourself from junk mail.

Data breaches

Many web services and mobile apps require an email address for signing up. When you create an account, your email goes into a list. Companies know [how to send mass emails](#) — and they use this list for notifications and marketing materials. But the problem is that even large corporations suffer from security breaches. For example, in June 2021 personal data for [700 million](#) LinkedIn users was put on sale on the dark web. This database included email addresses, full names, geolocation records, social media accounts, and other personal information.

The problem is that you can't 100% prevent large data breaches like this one. But, if you suddenly started receiving dozens of spam emails, chances are, your address has been exposed. Websites like [Have I Been Pwned?](#) check if your personal data was compromised. These services work like search engines — just enter your email address and they will look through exposed data. If your address was found in a breach, you'll get a message like this one.



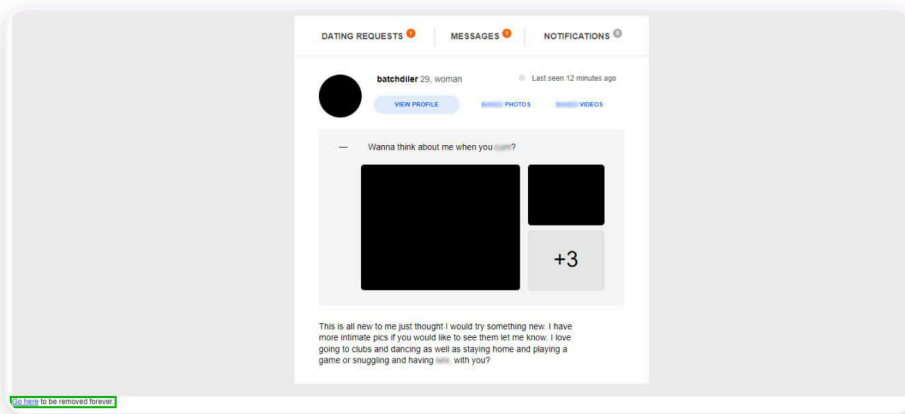
Accidental self-exposure

Data breaches are not the only source for spam mail. Spammers use publicly available information — users expose it themselves on forums and social media. For example, you wrote something like “Contact me at address@gmail.com” or made your address available for other users on a job search website — online activities like these put you at risk.

It's a less common technique now — spammers use leaked data more often. But you still can prevent self-exposure. To do this, change your privacy settings on social media and give your email address in private messages instead of comments.

Links in spam emails

Sometimes spam emails have the unsubscribe link — like this one:



It doesn't have to be a button — in this case it's a barely noticeable link. But spammers use such links to verify that your email account is active. This information will go further — and you'll get spam bombed. Even worse, such links may lead to compromised websites that can be used for phishing or installing dangerous software on your device.

Clicking on unsubscribe links in spam emails or responding to them is dangerous. That's why if you come across a suspicious email, just delete it from your inbox. You can also flag such emails as spam if the filter didn't catch them — this will protect you from receiving more emails from the same address.

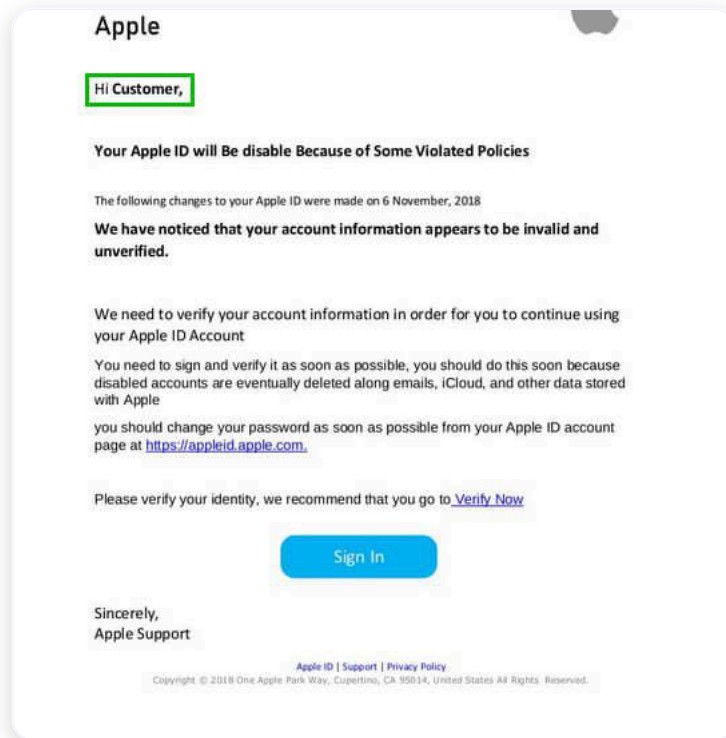
Most popular phishing and spam examples of 2024

In March 2021, spam emails accounted for [45%](#) of total email traffic — and most of it is malicious like phishing, malware or ransomware. Junk mail is not only annoying — interacting with these emails results in financial losses and identity theft.

We've picked 10 most popular email fraud schemes you can find in your inbox. Some of them are old, others are relatively recent.

Verify your Apple iCloud ID

These fake emails from Apple ask you to verify your account because it was put on hold for various reasons. But it's a phishing attempt. If you click the link, you will be redirected to a fake Apple website that will steal your account information.



Source:Sensors Tech Forum

In this case, the generic greeting is what gives the scam away. Legit emails from businesses always start with your name or the moniker you used for the account.

You've won!

It's a type of "too good to be true" spam email. They tell you that you won a lottery or sweepstakes — and encourage you to share personal data to receive the prize. It's an old scam but there's a modern variation to it — notifications about winning the COVID-19 vaccine lottery. Take a look at this example:

Thank You for submitting your claims. This email acknowledges receipt of your details.

The NC COVID-19 VACCINE LOTTERY drawings are part of Gov. Roy Cooper's push to get more people vaccinated against COVID-19.

Currently, 49% of people in Mecklenburg County have had a least one dose of the vaccine.

North Carolina's lottery drawings are performed with a random number generator in which your number was selected.

We have been appointed a personal CLAIMS CONSULTANT to help facilitate your claims ASAP, You are advised to contact your claims consultant immediately with the following recommended info/documentation to initiate your claims.

1. Winning Reference Number
2. Full Name
3. Date Of Birth
3. Address
4. Mobile #:
5. Occupation
6. A Copy of your Identification (Drivers Licence, Passport or State ID)

Contact your Clams Consultant below with the above requested informations:

Consultant Name: Ryan Rogers
 Consultant Email: ryanrogers55@aol.com

After validation of your details requested above, Your personal CLAIMS CONSULTANT with NCDHHS officials will reach out to you via email or phone. Validatic process can take from 24-72hrs after submitting of your IDENTIFICATION DOCUMENT to your claims consultant.

Find more details about NC COVID-19 VACCINE LOTTERY [HERE](#)

NC COVID-19 VACCINE LOTTERY.

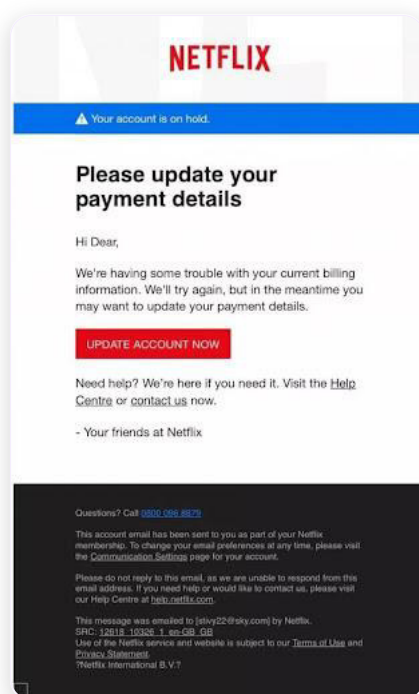
Source: WECT

These emails can be very convincing — COVID-19 vaccine lotteries actually exist. What gives the scammer away in this example is the public email domain — government officials have their own. If you received an email like that, look for public domains and spoofed addresses.

Missing information

It's another type of phishing scam. These spam emails claim that your account information should be updated or completed to avoid suspension. But once you click the link in the email, you'll be redirected to a phishing website.

Take a look at this fake Netflix email. That's a classic example of the "missing information" scam. The email asks you to update your credit card information — but the link leads to a fake website. To avoid financial losses, look for weird email domains like "netflix.corn".

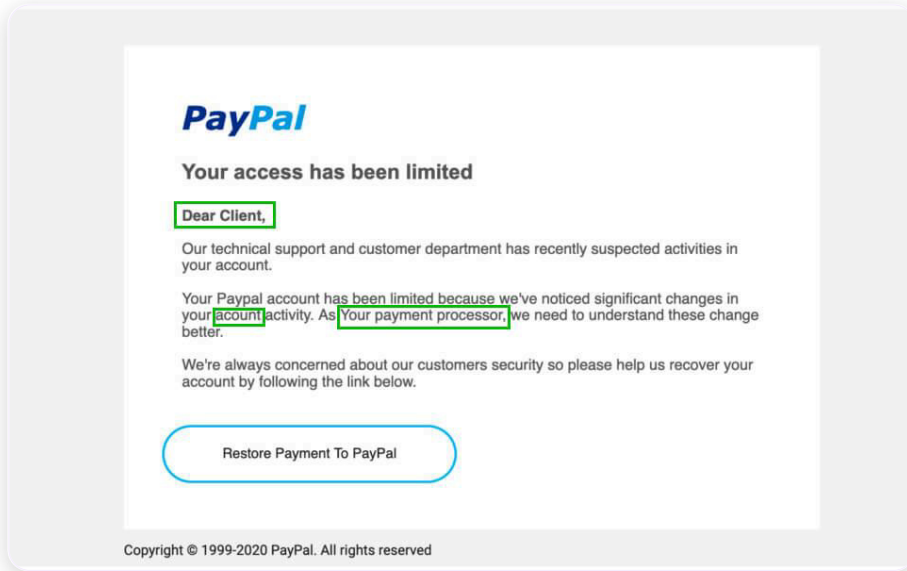


Source: Newsweek

Your online account has been locked

In this phishing scheme, spammers convince you that your account was suspended or limited for security-related reasons. To reactivate your account, you need to log in again using the link from the email. Then, like in other similar scams, spammers will steal your money or identity.

One of the examples is fake emails from PayPal — like this one:



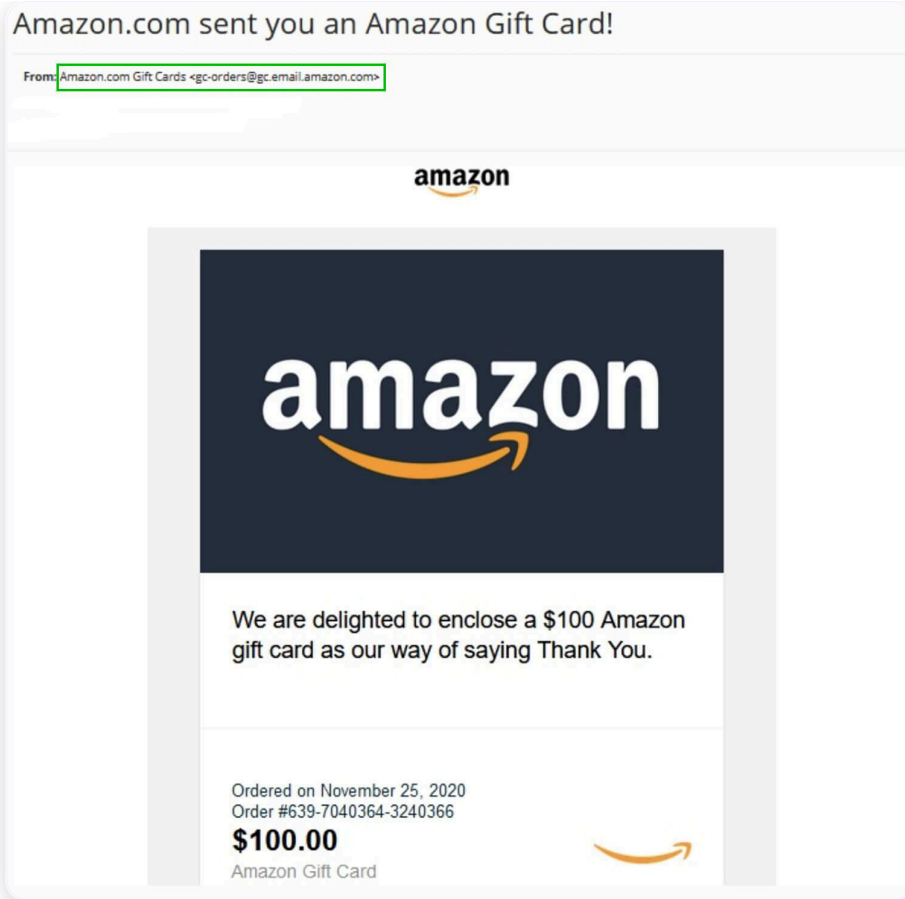
Source: Secplicity

You can tell it's not a legitimate email because of the generic greeting, spelling errors, and odd capitalization.

Claim your gift card

There are several variations of the gift card scam. Some emails ask you to send personal data to receive a gift card. Other messages have a link to a phishing website that will harvest your account information. But there are more complex schemes.

For example, this fake letter from Amazon has a "gift card" document attached to it. This file doesn't open but clicking on it installs Dridex — a trojan used for stealing bank account information.



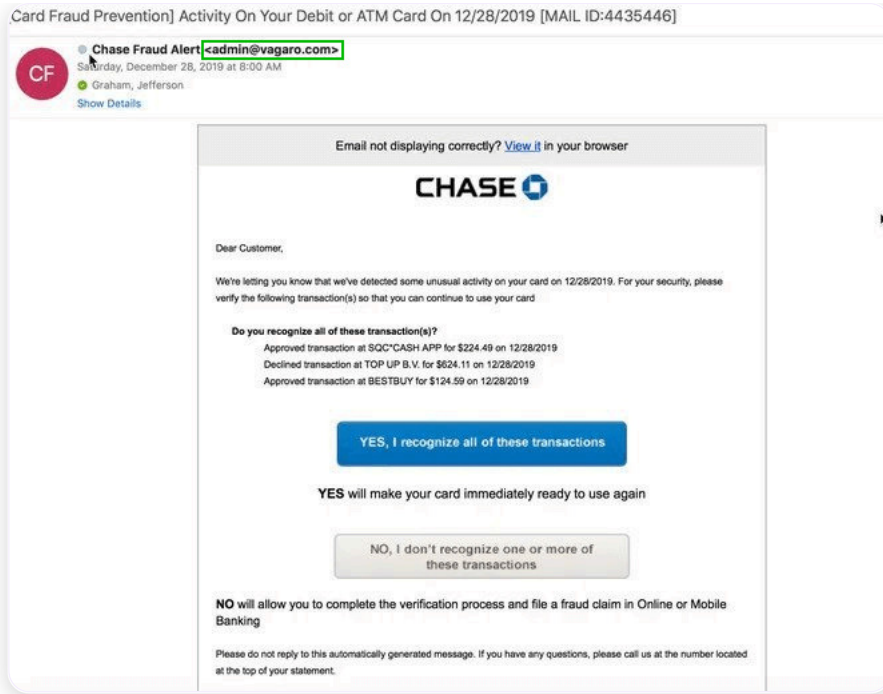
Source: The Sun

Take a look at the email domain — Amazon sends legit notifications from @amazon.com email addresses.

Suspicious activity with your bank account

It's another phishing scheme that is used to steal credit card information. You receive a fake fraud alert email where they ask you to verify your account on a fake website.

One of the examples is this email from Chase:



Source: USA Today

It looks legitimate but the public email domain gives the scam away.

You have a refund coming

This phishing scheme is basically sending fake government emails that promise you a tax return. The link in the email redirects you to a website that seems to be legitimate but steals your personal and financial information.

Fake tax refund emails can look like this:

HMRC - Notice

Dear xxx.com,

We are pleased to inform you that after the last annual calculation of your fiscal activity we have determined that you are eligible to receive a tax return of £3902.51

Description

Tax Return #8GB82761KZ

Issued Date: 13/09/2021 (08:00AM)

Expiration Date: 14/09/2021 (23:00PM)

Refundable Amount : £3902.51

United Kingdom

Note:

In order to receive your refund, you need to create a Government Gateway account and provide us the information needed to [receive your payment](#).

Currency

£

Tax Return #812823815955145

3902.51

Delivery: Electronically by Card

If you don't create a government gateway account, you will not receive your refund. This email was sent from a notification-only address that cannot accept incoming email. Please do not reply to this message.

Sub Total £3902.51

Delivery 0.00

Total £3902.51**Payment method:** Online

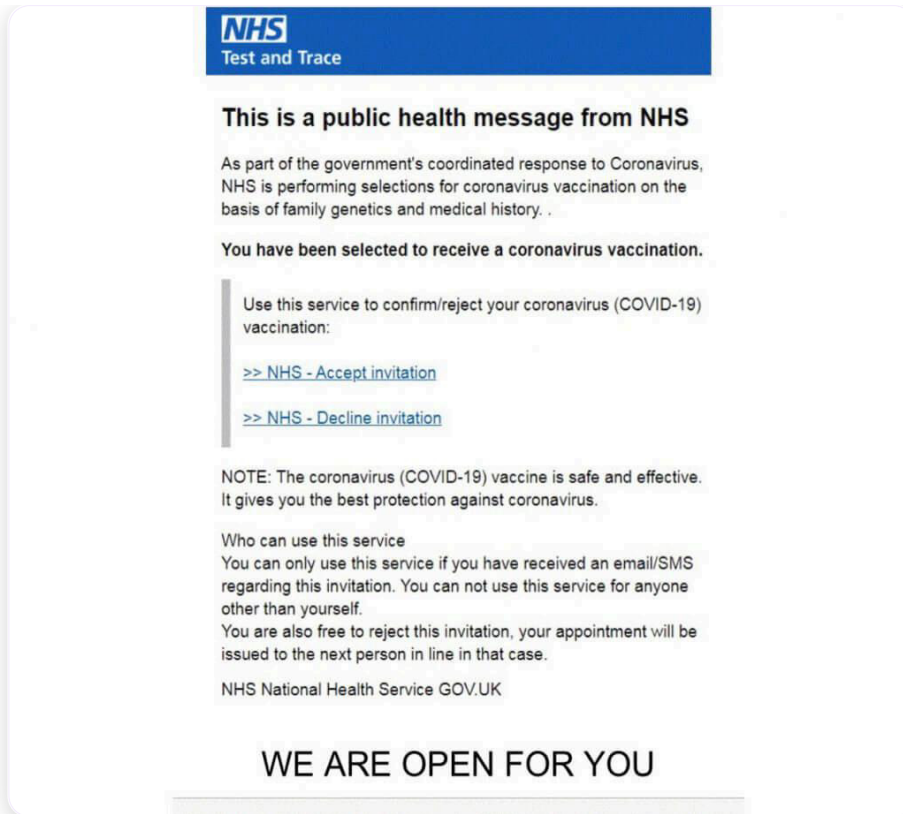
Source: GOV.UK

The official UK government website warns users that HMRC never sends email notifications about tax refunds. But if you live in a country with a different system, look for spoofed addresses and bad spelling to recognize a scam.

Get your COVID vaccination appointment

We already mentioned the COVID vaccine lottery scam — but that's not the only pandemic-related fraud scheme. For example, many people in the UK received fake emails from the NHS about paid vaccination appointments. The links lead to websites that collect personal and financial data. Government officials warn that the NHS distributes the vaccine for free and legitimate emails have different contents.

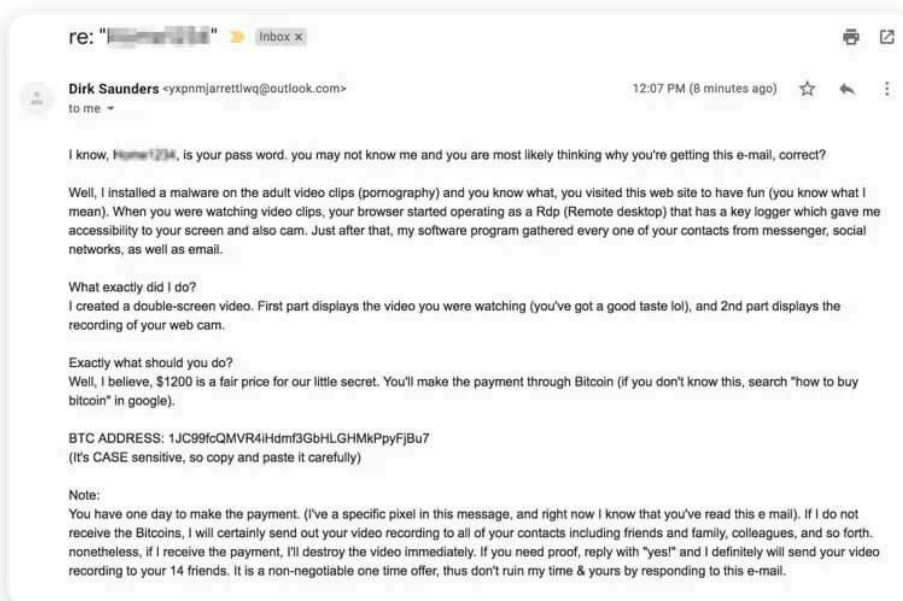
A scam email from the NHS looks like this:



Source: Newsroom

Bitcoin scams

There are many scams involving cryptocurrency — phishing, fake money giveaways, malware, fake exchange, and other schemes. Some of these scams involve emails, some don't. But one of the most widespread bitcoin-related spam emails is blackmail.

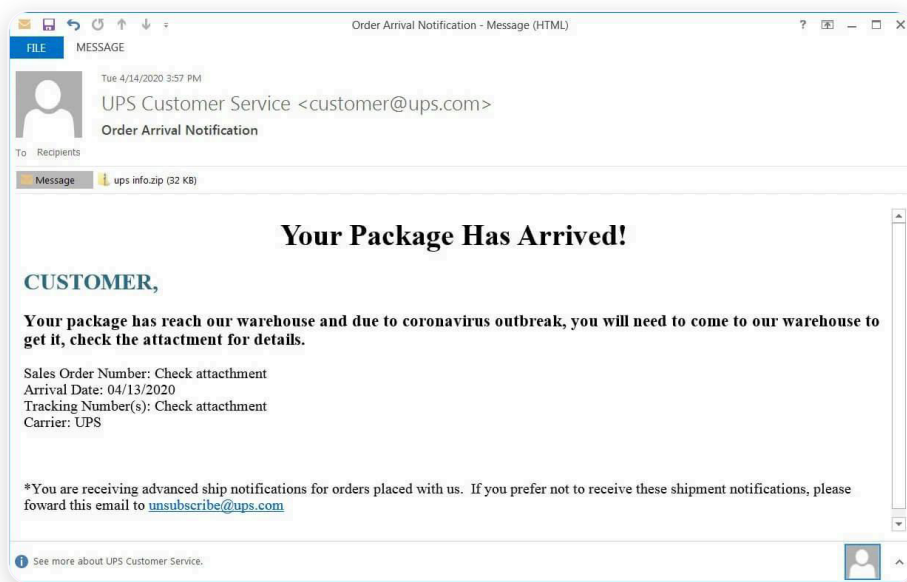


Source: Businessinsider

The sender claims that they hacked your computer, specifically, recorded a webcam video of you doing inappropriate things — and asks you to send them bitcoin or your relatives will see the video. And, although these threats might sound frightening, senders mention old passwords compromised by a data breach — so you probably weren't hacked. But, to ensure your security, use more complex passwords, enable two-factor authentication, and regularly check if your account was compromised.

You have a package delivery

It's a new phishing scheme that emerged during the COVID-19 pandemic. Spammers send fake emails from delivery services like FedEx or UPS — like this one:



Source: Bleeping Computer

They claim that your package has arrived at a warehouse but they can't send it to your house because of the outbreak. But if you open the attachment for details, you will catch a trojan virus that will have full access to your computer.

We didn't cover all the possible email fraud schemes — we listed 10 most common spam and phishing emails. But what if you received an email that doesn't fall under any of these categories?

How to identify a junk message quickly

Modern email apps have spam filters. For example, Gmail uses a neural net system that learns to separate junk mail from regular emails. But even AI is not infallible. Sometimes Gmail mistakes social media notifications or just emails with links and attachments for spam — and vice versa. That's why we give you 6 key features of junk mail to look for.

Suspicious email addresses

Pay attention to any unfamiliar addresses in your inbox. But just because you don't know it doesn't mean it's a spam email. Here's the list of red flags in email addresses:

- Random numbers and letters like ngoctrinh1403@gmail.com.
- Public email domain, especially if it's a message from an organization — gmail.com, yahoo.com, etc. Keep in mind that businesses use their own domains.
- Typos or extra symbols in a company domain like @amazonhelp.art instead of @amazon.com.
- "Donotreply" or other variations instead of the standard "no-reply" address for automated notifications.

But some spammers learned how to plausibly imitate corporate emails. If the address doesn't seem suspicious, take a look at the contents.

Personal data requests

Many businesses deal with personal data such as credit card information. For example, this is an email from Benchmark about cybersecurity concerns:



Hi Smiles Davis,

We're trying to renew your account, but keep getting billing errors. Don't worry, we've kept your data safe. Update your billing information today to avoid any account hiccups.

Fix Your Billing Details Now



How to fix it for credit card payments:

1. Click "Add a Credit Card"
2. Enter your credit card information and Click "Save"
3. Click "Upgrade" on the top right
4. Click "Continue" and then "Purchase Now"

We'll renew your account as soon as this new info is saved.



How to fix it for payments other than credit card:

[Contact Support](#) and they will help get your account reactivated.

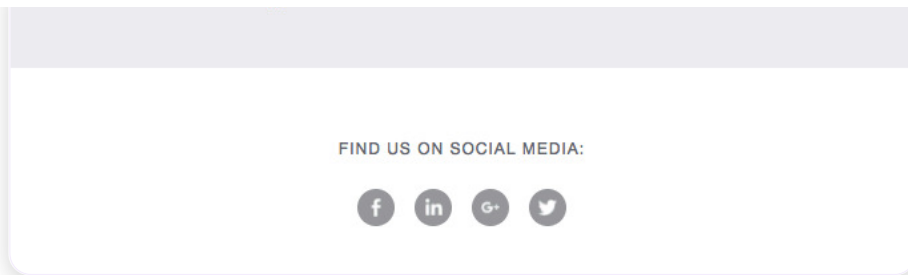
All the best,

Your friends at Benchmark

P.S. Questions?

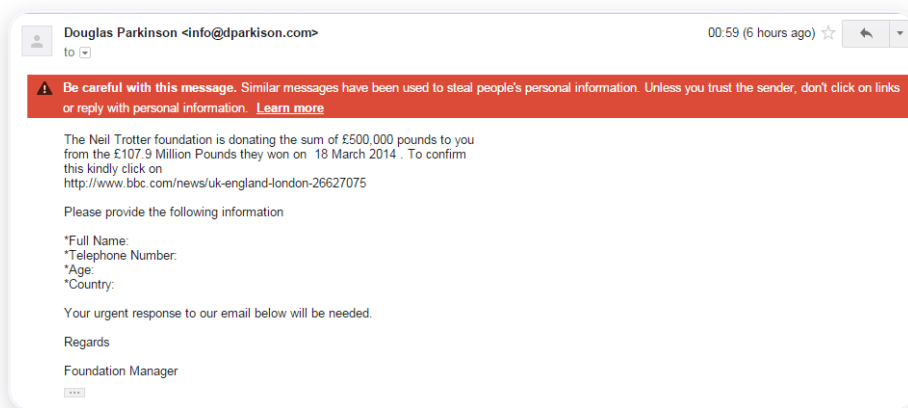
Please give us the opportunity to help.

[Contact our Support Team →](#)



Source: Really Good Emails

An important detail here is that Benchmark doesn't ask the client to reply with personal data. Instead, the sender asks them to fill in the necessary information on the company's website — unlike spammers:



Source: The Daily WTF

This example is an obvious scam and “Douglas” asks for relatively harmless data. But some spammers will ask you for credit card information or passwords. Keep in mind that, for example, bank employees will never ask you for the CVV code. That's why any personal data request, even as innocent as the one above, is a major red flag.

Sense of urgency

Creating a sense of urgency and appealing to FOMO is a common manipulation tactic in advertising. For example, take a look at this email from Barnes & Noble:

 FIND YOUR
LOCAL B&N

BARNES & NOBLE

VIEW IN
BROWSER

TIME IS TICKING

15% OFF

ANY ITEM EXPIRES SOON

ACTIVATE 15% OFF

Items Selected For You



Hello Girls, Hardcover

CHECK AVAILABILITY



NIV Our Family Story
Bible - Navy Wreath
(B&N Exclusive...

CHECK AVAILABILITY



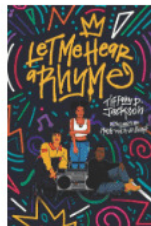
NIV Our Family Story
Bible - Rich Brown (B&N
Exclusive...

CHECK AVAILABILITY



Shark Lady: The True
Story of How Eugenie
Clark Became the...

CHECK AVAILABILITY



Let Me Hear a Rhyme,
Hardcover

CHECK AVAILABILITY

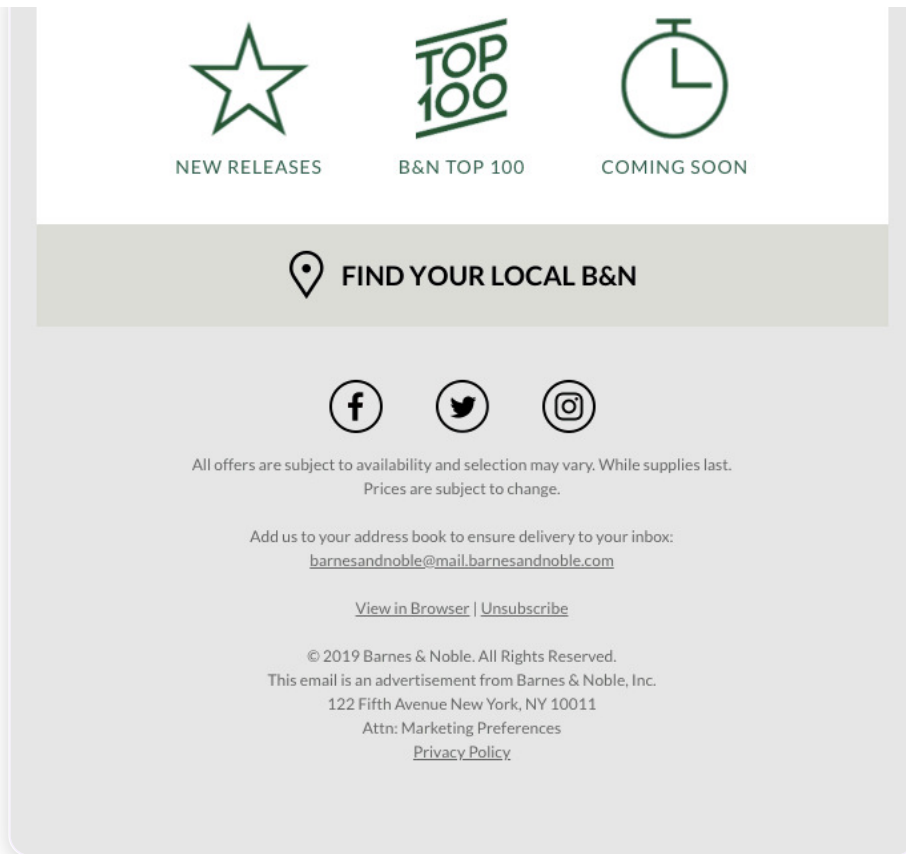


Top Ten, Paperback

CHECK AVAILABILITY

FREE SHIPPING ON
ORDERS OF \$35+

THE LARGEST ONLINE
BOOKSTORE



Source: Really Good Emails

In this email, Barnes & Noble offers a personalized book selection and a 15% discount that is active for a short time period. They use urgency since the offer is limited — but not like this:



This spam email uses an indefinite time period instead of the precise expiration date to create the sense of urgency, all caps, multiple exclamation marks, and too many words like “limited” and “offer”.. Such messages usually have clickbait [email headers](#) with the same words written in all caps and with excessive punctuation. Legit companies don’t introduce clients to limited offers using such blunt techniques.

But there’s one more sketchy detail — poor grammar at the end of the email. It brings us to the next junk mail feature — bad writing.

Typos and poor phrasing

When it comes to poor writing in spam emails, most people recall the infamous Nigerian scam. It started before the internet — people received letters from Nigerian royals or businessmen that asked for help with transferring money. Later it switched to digital and became more inventive with plots — for example, Nigerian princes turned into Russian entrepreneurs.

Take a look at this classic Nigerian scam email:

From MAUREEN UDAENU <mauda_2@yahoo.co.uk>:

Good Day Dear,

Am sorry for the inconveniency it may curse you for using this opportunity to communicating with you for the first time. Well I shall be extremely happy if you will kindly understand the content of my proposal thereby contributing your own quarter.

Its true that the message will have some characters, but I want you to choose the best character that should favour us better, so that we should forge ahead in this transaction .

Well I am Miss. Maureen Udaenu , and an indigene of G/Bissau, though I left my country as a matter of death scallating because of wars but that was not my primary aim of leaving my country to Dakar Senegal where I am currently staying now, my major reason is because I was humiliated by my late father's relatives as a result of their much focus on material things. I left my country because I was the only child left in my late father's lineage and It will not come to an end rather I will ensure I keep the family name on constant remembrance and existing.

But the principal aim for my being here is to concentrate well on what I will do in future with the money my late father left in one of the banks in Europe, the money is Five million eight US dollars (\$5.8 M).This money was meant for his multi investment projects before death struck him down. This is the principal reason why I am here in this country so that I shall concentrate and be mindful to this everlasting opportunity I inherited and to search for one who will stand on my behalf in the claim.

My contacting you is based on your complete capability to move to the Europe bank as soon as you could so that you will have a Table discussion with the bank thereby reclaiming and retransferring this money to your own bank account where it will be confidently be secured for my future investment There are other things that we should discuss as soon as you write back because we need to round up every bit of this matter before all the bank details should be exchanged to enable us come to close end of the whole matter which will lift me up from here to your country with your help and where we should stay for our investment projects as we agreed in the next page. Don't forget that there are some hidden percentage that I have wholeheartedly mapped for you which will be revealed when we come to agreement that you will help me to secure this money in your own easy accessible bank account.

Hope to hear from you and it will sound better and encouraging if you will reply with your complete data's so that I shall commence all applications on the need able documents that will ease the direct recommendation and also empowering you as my foreign live partner or my late father's business associate before his death.

Regards:
Miss. Maureen Udaenu.

Source: ResearchGate

Nigerian scam emails were poorly written to look more convincing — their senders didn't speak English as their first language. But other email scammers also write with typos, extra blank spaces, and odd phrasing — for different reasons:

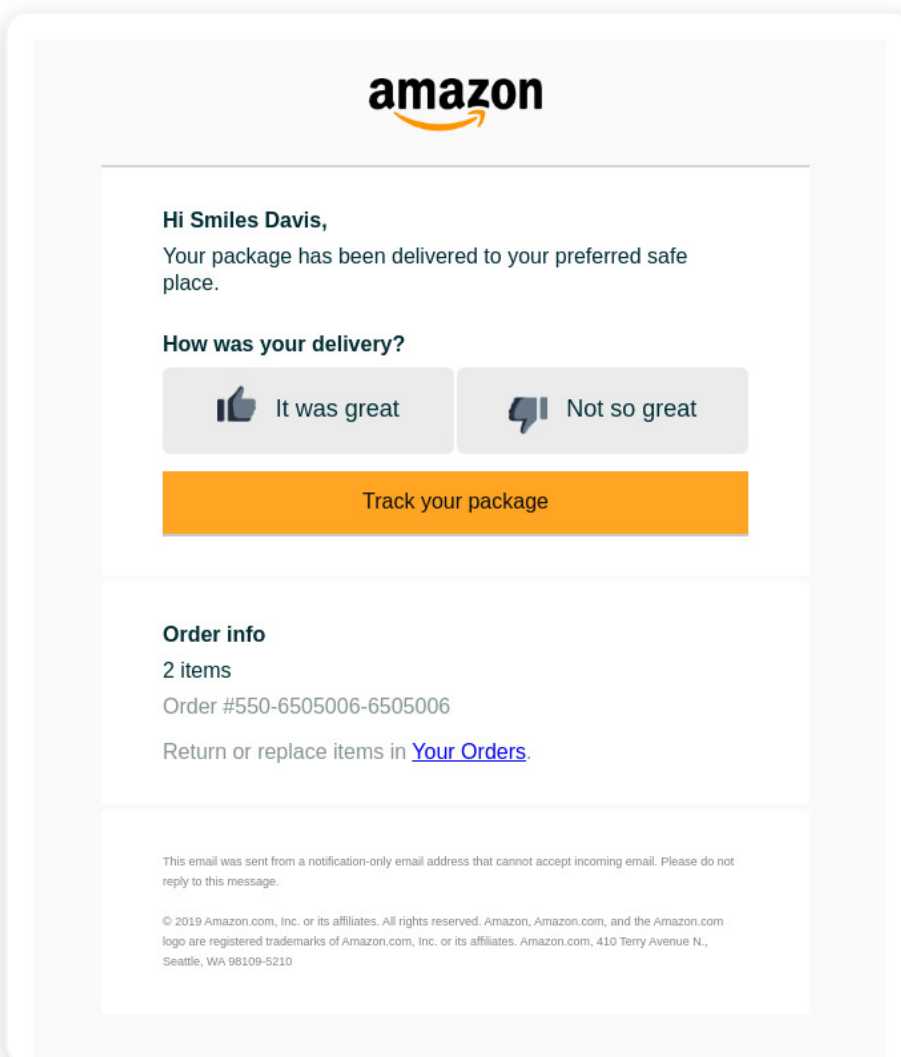
- **Tricking spam filters.** It doesn't work with modern spam filters — but historically spammers deliberately misspelled words so they could slip into your inbox. Now poor writing triggers AI-based filters instead of fooling them.

- **Machine translation.** Weird syntax and word choices might be the result of bad machine translation. If scammers appeal to a larger audience, they won't spend time writing messages in different languages from scratch.
- **Filtering the audience.** Cormac Herley, a researcher from Microsoft, suggested that bad grammar and comical stories in Nigerian scam emails are designed to [filter their readers](#). Smarter people won't sit through an email full of typos — but the most gullible audience will.

But the email above has another interesting detail. "Good Day Dear", aside from weird phrasing and capitalization, is also impersonal — that's another feature of spam emails.

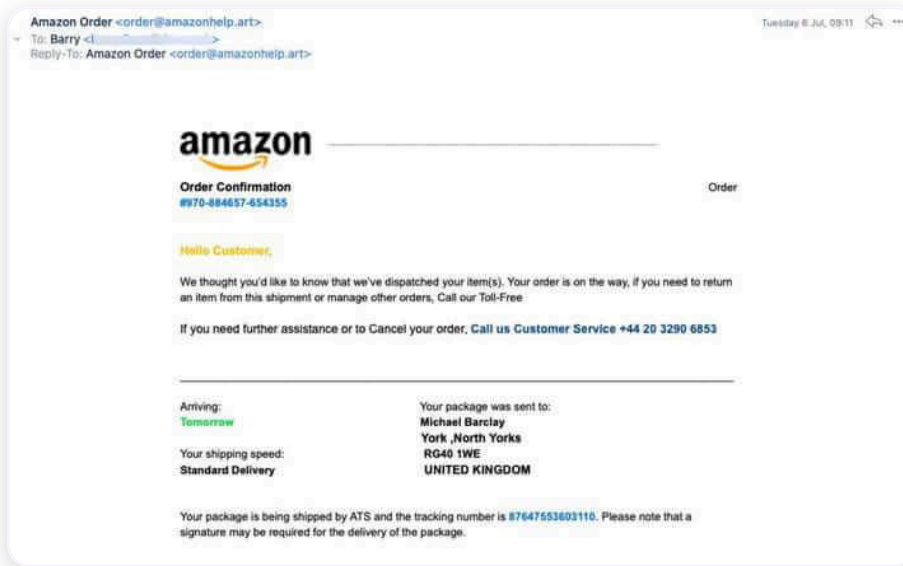
Impersonal delivery

According to Campaign Monitor, personalized emails increase sales by [20%](#). And personalization is not only about data-driven customization of offers — it's also about the language. Businesses include clients' names even in formal notification emails — like this one from Amazon:



Source: Really Good Emails

Spammers can imitate such notification emails in a pretty convincing way — except for one small detail. Compare our previous example to this fake Amazon email:



Source: Forbes

Even if fake emails imitate notifications from large companies, they have generic greetings like “Dear Customer/Client” or “Dear Sir/Madam”. But this, like the features we mentioned earlier, is a technical characteristic. What about the actual contents?

Too good to be true

Some spam emails will promise you a reward for clicking a link, downloading an attachment, or sending personal information. It can be a ridiculous amount of money or any other bonus from a company or even a celebrity. But the thing is, if it's too good to be true, chances are it is. For example, this email is definitely not from Mark Zuckerberg.



Source: Essential IT Solutions

These are the most prominent features of junk mail. If you come across any of these in the new email, do the following:

- don't click on any links, download attachments, or respond;
- mark this email as "Spam" so you wouldn't receive more junk mail from the same sender — or delete it from your inbox

Wrapping up

Spam emails might seem funny and clumsy but they are dangerous — phishing leads to loss of money and possible identity theft. Scammers get more inventive with their schemes — that's why it's important to know the key features of junk mail and never interact with such emails for the sake of your safety.

Some of the common spam emails are:

- Fake Apple ID account verification
- "You've won a lottery"
- Missing account information emails
- Account suspension
- Fake gift card claims
- Fake tax refund notifications
- Fake COVID vaccination appointments
- Bitcoin-related scams including blackmail
- Fake delivery notifications

And if a suspicious message doesn't fall under any of these schemes, you can use our checklist to make sure it's a spam email:

- A spoofed email address
- Requests for any personal data
- Sense of urgency
- Typos and poor grammar
- An impersonal greeting
- Too good to be true

Article by



Daria Zhuravleva

45 articles

I'm a writer with 3 years of experience, knowledge and interest in all things IT and marketing, and a passion for the English language. As a staff author at Selzy, I see my mission as an educator who makes your life easier by explaining complex topics in a digestible and somewhat entertaining way. Hobbies include birdwatching, all things music and art, writing freeform poetry, and hiding in the woods.

Visit Daria's

[Previous post](#)**Best Email Marketing Campaign Ideas To Get Inspired By**[Next post](#)**Choosing the Best Font for Email Marketing Campaigns**

Latest Articles



by Kate Shokurova

Starter Kit

Effective Email Marketing Strategies and Tips for Successful Campaigns

22 June, 2024 • 1631 views



by Alexey Baguzin

Starter Kit

How To Migrate to a New Email Service Provider

21 June, 2024 • 5 views



by N

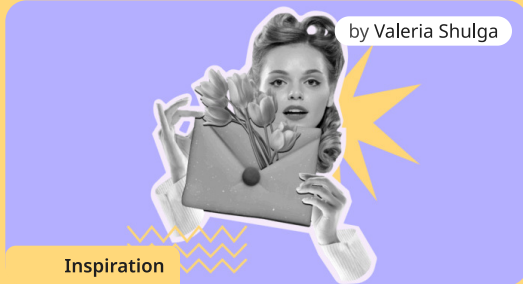
Tips and Tricks

A Comprehensive Guide to Email Localization in Marketing

20 June, 2024 • 152 views

[See more articles](#)

Trending



by Valeria Shulga

Inspiration

International Women's Day Email Inspiration & Best Examples To Follow

01 March, 2024 • 52434 views



by Ana Balashova

Inspiration

10 Most Important Email Marketing Trends That You Can Focus on in 2024 Year

21 January, 2024 • 43088 views



by Sara

Tips and Tricks

10 Best Temporary Email Services in 2024

24 August, 2023 • 41989 views



The Foolproof Guide To Email List Building

Others just make a list of ways. We actually explain how to make the most of each way.

21 surefire ways to grow your email list with detailed explanations and hand-picked examples. Based on research and **10+ years experience** in email marketing.

☐ I have read and agreed to [Privacy Policy](#). By entering my email I agree to subscribe to the email marketing digest by Selzy.

Selzy



Company

About Us

Careers

Prices

Knowledge base

Blog

Integrations

API docs

Brand Book

Sitemap

Features

Bulk email service

Email builder

A/B testing

Email analytics

Pop-ups

Segmentation

Automation

Triggered emails

Legal documents

Terms of use

Anti-spam policy

Privacy policy

GDPR

Cookies Policy

Refund

Bank accounts

Bug Bounty Program

Contacts

support@selzy.com

Ask us anything

US

+1 (929) 235-12-93

▼

© 2021–2024 Selzy