DISPOSABLE EMAIL ADDRESSES

Updated August 2019

Do your customers connect without making real contact?

WHO USES DISPOSABLE EMAILS?

There's a rising trend in the use of disposable emails for day-to-day digital life, with growth driven by online-shoppers and consumers.

STOPPING SPAM AND FRAUD

Email scams and data security breaches have fuelled the fire for burner email addresses. people want to protect their 'real' inboxes.

THE RIGHT TO BE ANONYMOUS

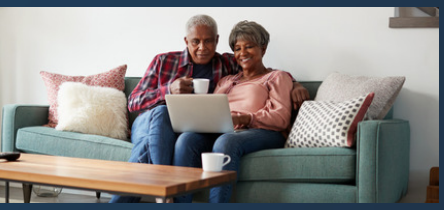
Data surveillance and the normalisation of supplying personal data online encourages people to opt for anonymity.

How does your business deal with disposable email addresses?

Are you cool with burners?

Disposable email addresses enable people to stay anonymous online. That's no bad thing. Not everyone who wants to be anonymous is doing anything wrong. Maybe you just live in China and want to watch Netflix.

But business owners have the right to decide whether to engage with people who will disappear behind a temporary 'burner' email address. What does your business need to know about them?



Since 2015 we've curated a list of temporary email address domains and shared it for free as a community tool. In addition we compile data daily on disposable email addresses and use this as our live filter for our email verification API.

From over 4,000 domains on the public list we took a random sample and checked out each one. We wanted to learn about the activity type of domains associated with temporary email address provision.

We didn't expect to find many angels on the list but the results surprised even us. Domains that have been providing temporary emails change purpose. The majority of them become inactive once they've been listed - they stop being used once they aren't hidden.

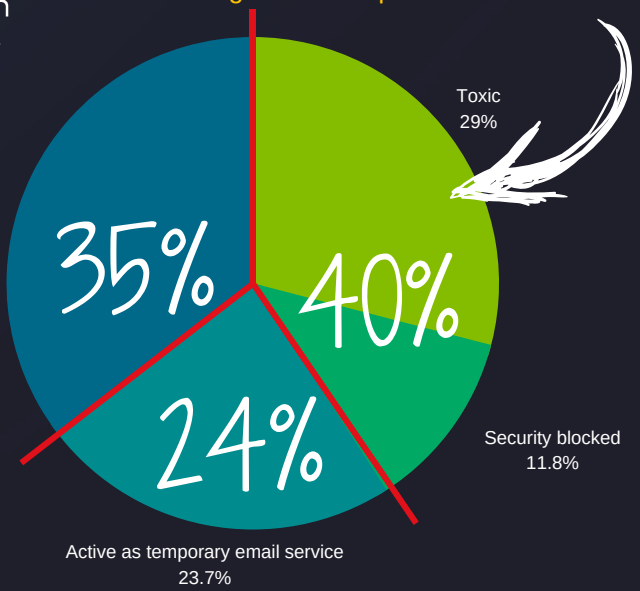
Of the domains that remain active the majority (>75%) carry toxic content, hide behind security blockers or are used as parked domains likely to be associated with fraud.

We think this evolution from temporary to toxic is an indicator of the original purpose of many temporary email providers as a tool for fraud.

The lowdown on disposable email domains

TOXIC OR SECURITY BLOCKED DOMAINS

Just over 40% of the domains we checked were either carrying toxic content (phishing scams, account takeover scams etc.) or we were blocked from accessing them - not public domain content.

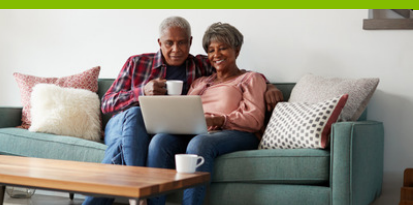


PARKED DOMAINS

Just over 35% of the domains we checked were parked domains. Many were linked to a common source. We've found that parked domains are disproportionately connected with fraud.

DOMAINS OFFERING TEMPORARY EMAIL ADDRESSES

About 24% of active domains offer temporary mail services. Of these, only one offered a non-technical user experience. The use of disposables may be rising but this environment is no place for IT innocents.



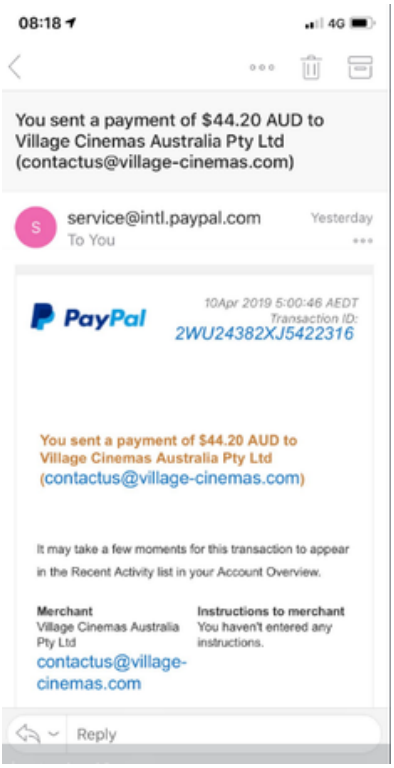
Using a disposable email address to stop spam and fraud

Nobody likes spam. It can be frightening and threatening and it's getting more convincing. That's why people are using temporary email addresses to prevent their 'real' email address being hacked, sold and shared. According to the go-to site for checking personal data security, 'haveIbeenpwned.com' there are now nearly 8 billion stolen email addresses in circulation.

The irony is that disposable email services are used by fraudsters too. When people start using a disposable address they could be exposing the contents of their temporary inbox to fraud. For example, two well known, free, temporary email providers are Guerrilla Mail and Temp-mail. You'll see these two recommended in mainstream publications and consumer affairs forums. Yet their privacy policies make it clear no temporary email is private and content can be read by any other user.

There's a world of difference between the compliance of mainstream email providers and temporary email address providers. We're not suggesting that every inbox is an encrypted, private sanctuary; after all, inbox scanning for keywords is a hot topic. It's fair to say that consumer expectations of security are probably higher than the terms offered by free burner email providers.

Real marketers don't send spam. But the 'report spam' button gets hit for forgotten newsletter signups, forwarded content from friends and legitimate contact about purchases. Data security is a hot news topic all day long and 'everyday folk' who want to buy online or download assets without giving away their real email address are increasingly turning to disposable email addresses. So where does that leave the marketer?

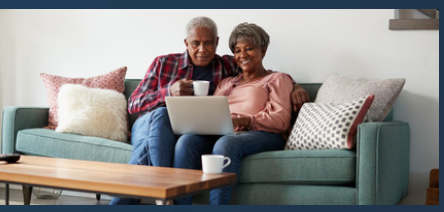


A sophisticated PayPal phishing spam attack
shared by @troyhunt
www.haveIbeen pwned.com

Marketing and burner emails

Marketers should always remove disposable emails from their data. **From 2018/19 we've seen a 100% rise in the use of bad email addresses supplied to marketing companies. And for the retail sector, the use of disposable email addresses has increased by x 10.** There' s no point mailing to a disposable email address. It will hard bounce. It will impact your sender reputation. If left to accumulate burner email addresses will distort your reporting and then mess up your planning.

HOUSTON - DO YOU HAVE A PROBLEM?
If you see a marked increase in the number of customers using burner emails you need to ask what their motives are. Are they trying to commit fraud, or is it just that they don't trust you? Listen to what the disposable users are 'saying' and take the opportunity for you to review your 360 user experience and check out your trust levels.



The right to be anonymous

It's no surprise that the idea of online anonymity and guarding personal data has become attractive for more people. Your customers have a right to be anonymous. But can you do business with them effectively if they are?

Here's our example; we're sharing our web analytics with you. A significant number (but <10%) of people signing up to try our services use a VPN (Virtual Private Network). We block VPN trials as we like to be sure where our customers are and where their data is being uploaded from.

We block all signups from disposable email addresses for two main reasons. Firstly, we like to know whose data we are processing and we want to be able to have an ongoing communication with them so we can update any terms of service. Secondly, we keep our fraud exposure at a minimal level. As a SaaS provider we're vulnerable to online fraud. In fact, when we began blocking disposable emails, we stopped over 80% of transaction fraud and chargebacks. That's a broad brush view of our anonymity policy. What's yours?

If you provide services that require identity verification, or you sell online in one of the high risk channels such as travel, leisure or SaaS, we think your policy to restrict anonymous, untraceable customers should be tight.

Disposable email addresses and Email Hippo

A summary

- We track, gather and share disposable email domains
- Our list cleaning service identities disposable emails
- Our API provides the intelligence to support
- business decisions
- Since April 2019 we have seen the use of disposable email addresses rise by 21%
- In the retail sector, disposable emails are used 10 x as often as they were in 2018

Conclusions

- Never keep disposable email addresses in your data
- Decide how you do business with people using disposable addresses
- Learn to adjust your user experience if you need real connections with real people

Want to learn more? Download our infographic series:

Why do people use disposable email addresses?
Are disposable email addresses good for business?
The pros and coons of disposable email addresses

emailHIPPO