techradar pro IT INSIGHTS FOR BUSINESS

US Edition ▼

Subscribe ▼

Windows 365 Latest Mobile news Microsoft Teams updates Linux at 30 Best hybrid

Home > News > Computing

How to shut down a phishing operation in 48 hours

By Fernando Cassia about 21 hours ago

And you can do it, too, even without Gmail’s help

(Image credit: Pixabay/Tumisu)

The software industry's response to phishing has previously been centered mostly on flagging fraudulent email messages. But that is a shortsighted view, not to mention a slow process.

According to the FBI's Internet Crime Complaint Centre (IC3), phishing accounted for 30,48% of all received complaints in 2020, making it the area with the highest victim count. Around the world, authorities are busy alerting the public to be extra-paranoid to not click suspect links. But what about the criminals running the websites - how is it possible that scamming operations often run for days, if not weeks?

Here's my recent experience on shutting down one phishing operation over the course of two weekend days, and how the IT industry as a whole could improve its act.

- Check out our list of the best identity theft protection around
- Here's our list of the best endpoint protection software
- These are the best firewall software and services

Why the current "solution" is incomplete

Most webmail sites offer one way or another of flagging a message as phishing. In Outlook, for instance, it's above the reading pane, where you can select Junk > Phishing >

Report. In AOL you have little option but to just flag it as "junk". In Gmail it is called "report phishing" - if you can see it* depending on the Gmail version you are seeing (but more on that later).

Supposing you do realise an email is indeed fake, click on the "report" option and get a false sense of virtue - a virtual "mission accomplished" banner flies across your mind and you forget all about it. You might think that this email now goes into a central database from your provider, and as soon as a certain threshold is reached, all further emails are “automagically” flagged as Spam, identified as "Potential Phishing" with a huge banner displayed at the top, or not delivered at all, depending on the policies of the email provider.

But what about the website that was luring victims? Well, it keeps running, waiting for more victims. Victims who could in fact be using *other* email services without access to such reports, like company/personal email domains and the like where the messages will just come straight to inboxes. So, as far as the perpetrator is concerned, flagging the emails as phishing only slows down the speed of the spread of the message, not its honey pot and central repository of stolen information.

Details of the incident

This author was confronted with such questions back in May 2021 when he encountered a phishing email up close and personal.

As you will see, the phishing operation's website ran in Chile, but targeted people in neighboring Argentina by impersonating the country's Social Security Administration, ANSES, preying on the vulnerable and promising a new payment of government-issued COVID relief funds.

The legit-looking website sported the same headers and typeface as the official government web page, but with a little extra detail: a “dot shop” junk TLD domain name.

The fake web site impersonating Social Security - a dot-shop domain name should raise all the alarm bells. (Image credit: Fernando Cassia)

Predictably, the purpose of the whole exercise was having your enter your debit card "to receive the benefits" (Screenshot edited,translated from Spanish) (Image credit: Fernando Cassia)

Gmail’s answer to phishing? From good to terrible

(Image credit: Fernando Cassia)

User interfaces are a very important part of the fight against phishing, malware, and everything related to *infosec*. If you complicate things, people won’t bother to report the messages, won’t follow correct procedures, and won’t read the warnings.

The lack of coherence in GUIs can be painful. In the words of California lawyer-turned-consultant Bruce Berls rant against Win10’s disappearing scroll bars, *“so each day you start drinking earlier in the afternoon and before long you’re pushing small children down when no one is looking. It’s a sad story”*.

Google has a similar infuriating annoyance in Gmail, a service with *four* different user interfaces of which there’s a correct phishing report button in **one**: It’s a recipe for disaster.

Gmail’s desktop interface is the only one that at time of writing includes a separate option to report phishing. On the rest you can only flag messages as Spam, the least useful of weapons against phishers, as there is no report of the incident for later analysis.

To add insult to injury, two useful options *“Download message”* and *“Show Original”* which are very useful for sending phishing reports to authorities using web report forms, are noticeably missing from the Gmail Android app.

A certain lack of coherence: in Chrome for Android you can load three user interfaces. Only one passes the test with regards to phishing reports. (Image credit: Fernando Cassia)

As things currently stand, if you want to properly report phishing from Gmail you have to load it in your mobile browser. But there are three versions of the Gmail site, and only in the desktop version you get an individual option correctly labeled “Report Phishing”. In other browsers, the only option is to flag the message as Spam. If you count the Gmail for Android app, that’s o*ne out of four.*

To further complicate matters, the only way to switch among user interfaces in the Gmail web page is by clicking on the often missed page footer where you can tap and select between HTML (correctly labeled “old version” and very useful for slow mobile connections), a more stylish lightweight “Mobile” version, and the full blown Desktop version. For the latter to load you need to go to the browser’s options menu, and select “Desktop Site”. Predictably this loads slowly, as it was not designed for mobile screen sizes and slower processors, but the Workspace view - as Google likes to calls it now - is the only way to get the elusive “report phishing” button.

Gmail for Android - The phisher’s favorite

In this case, the phishing email arrived in my Gmail inbox, and I read it on my Android mobile device using the official Gmail app - probably just what the phishers wanted, as Google has a lot to improve in this area.

For starters, if you use the Gmail app, by default you don't see the sender's email address, just its "name". Surprise! The phishers put the known firm's name there, even if the email address is actually gibberish12345@gmail.com. So you see *"Familiar name"* not "gibberish12345@isp" which would be a big warning sign for most.

Hiding the sender’s email address. A very bad idea (Image credit: Fernando Cassia)

Certainly you’d know one father, sister or friend who might have fallen for any such legitimate-looking email, especially with the address hidden.

The solution? War.

What an IT and programming education teaches you is how to turn every complex problem into a series of small problems, and tackle each one step by step - thus solving the big problems effortlessly.

What follows is a succinct account of the small steps taken in my battle with the phishers, including screenshots of each step, so you can hopefully do the same.

First (and hopefully obvious) move: report the phishing email message to Google.

This helps Google flag the received message as unsafe, and if all goes well, it's less likely to turn up in someone's search results in the future.

(Image credit: Fernando Cassia)

But even that alone is a big "IF", as most victims just click on a URL they receive by email, WhatsApp, Telegram or other means. And if you received it, thousands of others will probably have also received it. Time is of the essence - are you going to rely and trust on a cloud algorithm to "prioritise" it right automatically? I wouldn't.

Google’s Safebrowsing report form. Time to type. (Image credit: Fernando Cassia)

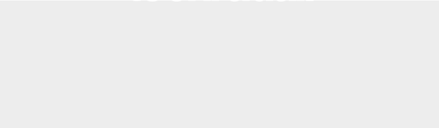
Google's "Report Phishing" web page can be found at the safebrowsing.google.com domain, here. Report the target URL you were sent to by ~~clicking~~ copy-pasting the link from the email. End of ***Strike one***!

Second move: Going after the email sender in every possible way.

As mentioned, it's almost unforgivable that Gmail's Android app makes things easier for the phishers by hiding the sender's email address. So regardless of your email provider, if you find its “Report Phishing” option, or you use an email client that has an option to flag an individual email as phishing, by all means do use it. ***Strike Two!***

As an additional step, you can also report a message manually to the email provider's abuse team to have the account terminated. Be prepared to fill out yet another web form, manually. In this case the offender was a Gmail account so it was easy enough, as Gmail has an abuse report form in its support page here. End of ***Strike Three!***

This time and by pure chance, the email campaign included a SendinBlue -email infrastructure provider- footer, so I quickly mentioned it on Twitter. Luckily, someone from the firm was paying attention and told me they would hop on the case for analysis and termination of the account used for the mailing.



(Image credit: Fernando Cassia)

Strike four!.

As a final (nuclear) measure, you can forward the entire phishing email to the US CERT, at this address: phishing-report@us-cert.gov

(That would be Strike Five)

Yet it is worth remembering that even after these many manual steps, the fake website would still be live and collecting data.

(Image credit: Fernando Cassia)

Final Move: Sink that site.

For this step there are several tools which could be used, this is just the one I had at hand: Inspire Media's *HostingChecker.com* web tool. By pasting the offending domain name -in this case "anses.shop" - this reveals not only the obvious server IP address, but more importantly, the owner of that IP range. That is exactly what you need to find the company and report the offending site to them - which in this case was a Chilean hosting firm from the city of Curico.

HostingChecker: If there is an IP address there’s a company which owns that netblock (Image credit: Fernando Cassia)

Now it's where your luck comes into play. There are responsive firms... and those that are not so fast. Luckily, nowadays the world+dog has an online account at some social media platform - and I checked on Twitter and they were there. Chastising any firm in public always gets you a response - but this wasn't my lucky day, because it was a Saturday and the firm's community manager was surely enjoying some well deserved time off. So here's my next advice for the young - *Linkedin is your friend* - "use it you must" as Yoda would say.

I quickly found the company's founder and two of the firm’s IT guys, by name only. Now, if you are in a hurry and your house is on fire, or, if you're trying to **bring down a phisher's operation as quickly as possible**, requesting a connection to a stranger on Linkedin and waiting for him/her to approve you is not ideal. On LinkedIn you will get plenty of names which is a good start, but not so many emails.

To find emails of people you could start by asking in social media for any contact leads at the hosting firm, and message firms’ community managers privately. Or, you could do what I did out of desperation: googling "find 'person's name' email". The emails weren’t directly indexed by Google in this case, but I got an assorted list of sites which promise to give you *anyone's email address*. Some of these work. Some of these don't. The one I used did work wonders. Armed with the **names and emails** of people at the company, from the founders to a few employees of the hosting firm the only thing left is creating a convincing message, something that would be clicked on and read. Like the phisher’s do - but this time, for a good reason.

I wrote a polite email to the founder and CEO of the hosting firm - it’s better not to be nasty, I used an open question: "could it be possible that your $Firm is hosting a phishing site? *please check… thanks in advance, yours truly, have a nice weekend…*” and so on and so forth.

Understandably, no firm’s CEO would want to see the company's name associated with phishing or any nasty stuff, so a subject line like that will get their attention. My odds were low as it was during the weekend, so I couldn't count on the founder reading email from a total stranger on a weekend. A second message to anyone in IT operations helps. Mine read "A customer of yours is hosting $domain for phishing" straight from the subject line. In the message I mentioned in passing that *the founder and CEO were contacted about it too*. That should get them moving. But the larger the corporation, the harder it gets to get the "people who know", so your mileage might vary. But with the Emails sent that's... ***Strike Six!.***

The next day, to my surprise, a reply showed up in my inbox. It was one of the techies at the Chile-based hosting firm, thanking me for the report and promising it would be shared with the operations team.

(Image credit: Fernando Cassia)

A couple hours later, the domain had completely vanished from the web. So kudos to them for acting fast. Knocking on every door really does pay off - and if you want to bring down a phishing operation, you can do it too. Just don't quit after the lazy *"report spam"* click, as it amounts to nothing in practice..

Conclusion: IF ONLY it was automated!.

In the age of "machine learning" and AI, one would expect the software industry to have agreed on some degree of interoperability with regards to its abuse reporting systems by now. The web browser firms, the email service providers, the web hosting firms AND the web domain registrars all are parts of the problem. Flagging emails as junk or phishing do NOT shut down websites.

It wouldn't be exactly rocket science to devise a way for web browser users to report, with a single click, such instances of nefarious web sites, have the sites *"Automagically"* analised by machine learning models to to notice and discriminate the true web sites from the fake, the official domains from the totally bogus, AND have the abuse teams at hosting and registrar contacted, in a single step.

Going further, one possible mitigation step would be to get the domain registrars to be proactive rather than reactive. Since the main web targets for phishing are usually banks, financial institutions and government sites, how difficult would it be for Top Level Domain (TLD) registrars to keep a database of such "HIGH RISK" entities (brand names) and have domain registrars check new domain registrations against such flagged words?

To put it simple, if a Joe Something from Canada or Brazil or France registers a ***BankOfAmerica.shop*** domain, and "bankofamerica" is in a list of financial institutions, why can't the domain registrar put that registration on hold pending additional in-depth customer identity verification? That would be a good first step.

Until the browsers and mobile email apps continue to be "dumb" even in so-called "Smart" Phones, you will have to follow this long manual recipe of “knocking on every possible door” if you want to really go after phishers and nuke their operations in a timely manner.

- Stay safe online with the best VPN services around

Fernando Cassia

Fernando Cassia is a freelance Tech Writer living in Buenos Aires, Argentina. He has also written for Mike Magee's The Inquirer, Theo Valich’s BSN, TechEye, and other online publications. When he's not chasing Phishers, he's procrastinating on Twitter. Find him at @fcassia

SEE MORE COMPUTING NEWS ▶

Your Email Address

□ Contact me with news and offers from other Future brands

□ Receive email from us on behalf of our trusted partners or sponsors

SIGN ME UP

By submitting your information you agree to the Terms & Conditions and Privacy Policy and are aged 16 or over.

MOST POPULAR MOST SHARED

1 **PlayStation Showcase: all the PS5 game announcements as they happened**

2 **How to scan your face in NBA 2K22 – and whether you should bother**

3 **Your old Xbox One controller is about to get a lot more useful**

4 **There's been another huge quantum computing breakthrough**

5 **PS5 restock tracker for GameStop, Best Buy and Target dates – where to buy PS5 next**

TechRadar is part of Future US Inc, an international media group and leading digital publisher. **Visit our corporate site**.

About Us Terms and conditions Privacy policy Cookies policy Advertise with us

Web notifications Accessibility Statement