DNS ABUSE INSTITUTE

Making Phishing Reports Useful

Many service providers in the internet ecosystem are, unfortunately, recipients of phishing reports. This includes domain name registrars, resellers, and registry operators.

Phishing reports may be submitted by end users, internet security organizations, law enforcement, or other service providers. Depending on circumstances, providing a high-quality report may be the difference between a prompt successful mitigation and a delayed or ineffective response.

This best practice document attempts to provide a plain language description of phishing and help guide both reporters and report recipients toward the content that makes for a high-quality, actionable report.

What is phishing?

Phishing is an attempt to trick people into sharing important or sensitive information—for example logins, passwords, credit card numbers or banking information—in either a personal or business context.

So what does this look like in real life, and what facts might provide evidence to support mitigation?

One way to think about phishing is firstly in terms of an attempt to trick people, and secondly, in terms of the purpose of collecting credentials.

The attempt to trick takes place through some form of communication, often via an email, but sometimes via other media such as SMS or a calendar invitation, from a sender that is impersonating a trusted entity or person. For example, a bank, a company, a government agency, or even your boss. Frequently the message will also include some sort of 'call to action' –a positive or negative incentive designed to encourage you to act (e.g. reset your password, deny a transaction, claim a refund or a reward). It is possible for a phishing to take place without a distribution mechanism, but sending a communication to potential victims is a tactic used to drive traffic to the website.

Secondly, the collection of information often happens via a website asking you to enter your email address, passwords, or financial information. This website is often linked in an email, and often sent to a large number of potential victims. The goal is to obtain important information from the recipient of the phish. This information can then be sold, or used to defraud the victim (or the victim's employer). It could even be used to create further victims, for example, by impersonating that person. If the phishing attack targets credentials and the victim uses the same credentials for multiple logins, the impact can increase very quickly.

In some situations, a phishing message can be confused with a spam message. While it is true that all phishing emails or SMS messages are spam (that is, unsolicited), the inverse is not true. That is, not all spam messages are phishing. There are plenty of spam messages that, while both unwanted and annoying, are not designed to trick the recipient into revealing sensitive information.

Mitigation at the DNS level

Just as phishing comes in a variety of forms, the ways in which a domain name might be involved in phishing can vary. A domain name could be used to send an email, or it could be associated with the website that is collecting personal information, or both. But regardless of how a domain name might be used in phishing, it's important to distinguish between malicious domain name registrations and compromised domain name registrations.

A **malicious** domain name registration is one where the domain name has been registered for malicious purposes (i.e., to carry out phishing). Malicious registrations are generally more suited to mitigation at the DNS level than compromised registrations. A malicious registration is generally more likely to be a newer registration. The domain name is probably going to bear a close resemblance to the organization or institution the attacker is pretending to be in order to gain trust (e.g. the bank, public service, etc). The website associated with that domain name for a malicious registration is generally not being used for any other legitimate purpose, and it could be the same website used for the phishing attack.

A clear indication that phishing is associated with a malicious registration is where there is an obvious, unambiguous impersonation in both the domain name and the content on the website the domain name is pointing to. For example, the domain name could be confusingly similar to a government agency–perhaps HM Revenue & Customs (hmrc.gov.uk) in the UK, or the Internal Revenue Service (IRS) in the US (irs.gov). The website associated with that domain name would likely use convincingly similar branding, colors and style to the original official government website. This combination of a domain name and website that impersonate a trusted entity make it possible for an attacker to collect information from unsuspecting visitors.

Disabling a maliciously registered domain name at the DNS level is less likely to come with collateral damage (such as impacts on a legitimate registrant) and is typically more appropriate for DNS level mitigation, with the registrar being the first point of contact. All of this typically requires a report with sufficient evidence to justify this intervention.

A **compromised** domain name registration is a benign domain name that has been compromised at the website, hosting, email, or DNS level. Compromised in this context means that someone else has taken some control over their website, and/or hosting, and/or email, and/or domain name. Often compromise is the result of poor website security practices.[1] With a compromised registration, there is often an innocent registrant, who may themselves be a victim of phishing activity. If the website is otherwise being used for a legitimate purpose, taking action at the DNS level could result in unacceptable collateral damage.

Things get complicated when a compromise is present, because in certain circumstances the website is providing a useful, or even critical, service for the wider community. For example, if the website is the primary source of news information for a country or offers critical services for people in physical or mental crisis, suspending the domain name may cause more harm than the phishing risk we are trying to mitigate.

Disabling a compromised domain name registration at the DNS level is more likely to cause collateral damage and it is typically less appropriate for DNS level mitigation. The appropriate course of action is usually to refer the issue to the hosting provider or registrant for a more precise intervention and if applicable, a solution to the vulnerability that has been exploited. All of this typically requires a report with sufficient evidence to justify this intervention.

Providing sufficient evidence

If you encounter phishing, you can report it. We provide a free service– NetBeacon –to help make reporting easier. To make a report, we ask for specific evidence to be provided to help the registrar assess whether phishing is taking place.

The minimum information we ask for is:

- The **date** on which you encountered this harm
- The **name** of the company or organization being impersonated
- A **brief description** of the issue

[1] For more information on how to make sure your website is secure, see our previous article: https://dnsabuseinstitute.org/secure-your-website-save-the-internet/

These details help the registrar understand the behavior, assess whether impersonation is occurring, and provide context. The registrar may need to make a judgment call as to whether what is taking place is a breach of their terms and conditions, and if so, which course of action (if any) is most appropriate. This judgment call is not risk-free. Providing high quality information is crucial to help the registrar investigate and make a decision.

Ideally, it's helpful to provide some additional information:

- **Where** you were generally located when you encountered the phish
- The **website** (URL) of the company or organization being impersonated (if applicable)
- Any **screenshots** that might help an investigation
- If the phish was sent via email, the **sender's email address**
- The email message **headers** and the email message **body**

Phishing attacks can often be geographically targeted; trusted organizations and institutions are different depending on local context and knowledge. It's also useful to know where the phishing was encountered in case the registrar tries to verify the report and cannot reproduce the results.

If the phish is sent via email, it doesn't always come from the same domain name that is linked to the website being used to collect personal information. To help the registrar make sense of this, getting the email message headers and the email message body is very much appreciated. This step can be a little complex, so here is some information to help.

Email headers and message body

The trickiest part of this list is the email headers and message body text. This is different from screenshotting what is displayed when you view the message in your email app/client. It takes a little bit of work and the exact details vary based on the email app/client, but it is really important to those who research phishing reports.

Every email message is made up of an email header and a message body. An **email header** is the section of the email message that contains details such as a record of mail servers, time-stamps, IP addresses, sender and recipient information. It's sort of like the envelope of a letter. An email **message body** is sort of like the letter inside the envelope. It will look a little like the content of the email you see in your email client, but it is typically sent as a combination of raw text and formatting codes, for example any hyperlinks will be included in full (although unformatted "plain text" email does exist in certain situations).

These email headers and the “raw” source text aren’t something you typically see from just looking at the email in your inbox. The process for finding them is different depending on which email client (program/app/interface) you are using (e.g. Outlook, Gmail, Hotmail etc).

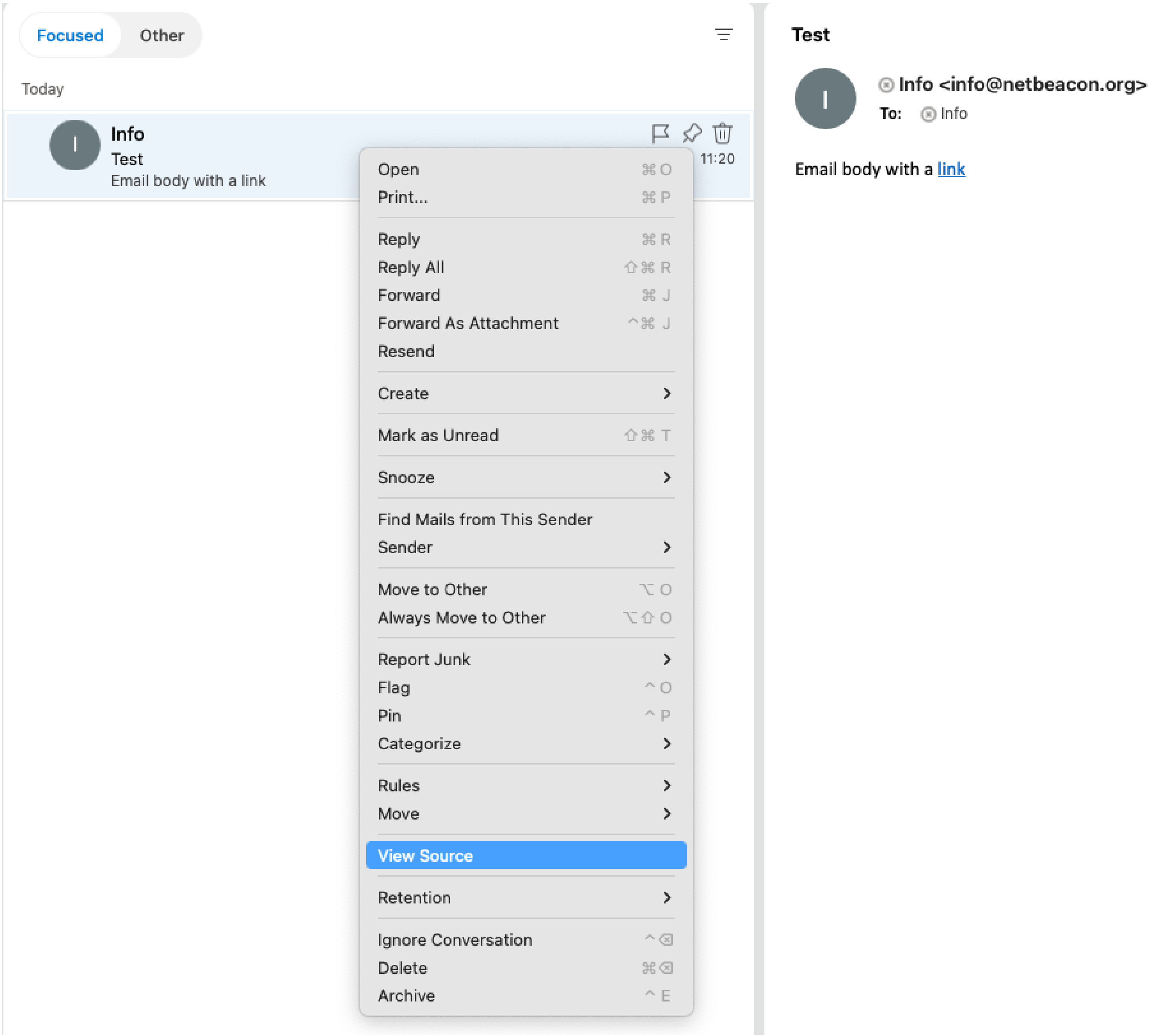
Finding this information will help the registrar understand where the email is really coming from and, if the email is asking you to follow a link, where that link is really sending you. Originating email addresses can be spoofed (faked), and hyperlinks can be disguised. The email header and message body will provide more information than is typically visible to the user.

To capture the email header, generally, what you’re looking for is an option (in your email client) to ‘view’ or ‘show’ the ‘source’ / ‘message source’ / ‘headers’ / ‘message details’ / ‘internet headers’ / ‘original’ / ‘raw source’.

This option lives in different places depending on your email client. You can try, right clicking on an email, going into ‘options’, clicking on drop down arrows (sometimes located next to ‘reply all’), or clicking the menu icon (perhaps three little vertical dots, three horizontal bars, or a 3x3 grid of small squares, depending on the client) for more options.

There are various guides online to help you with specific instructions. Sometimes a quick web search using the name of your email client and ‘get email header and message body’ will also help.

Example 1
In Outlook on Apple, right click on the message, then click ‘View Source’. This will open a new window with text in it. You can copy and paste the text into NetBeacon or take a screenshot.



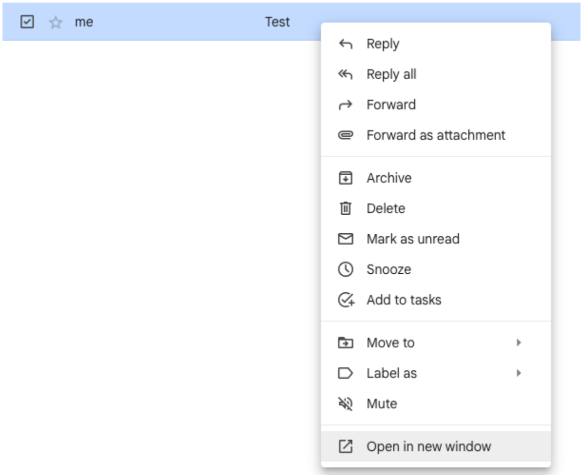
Info <info@netbeacon.org>

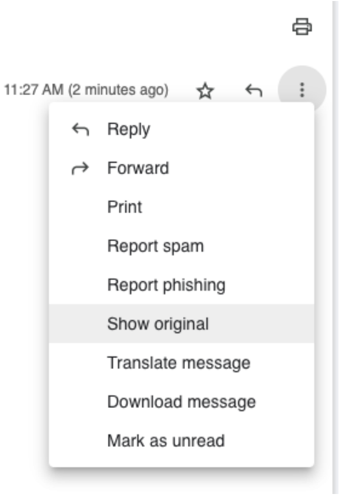
To: Info

Email body with a link

Example 2

In Gmail, you can right click on the email, and select ‘Open in new window’. Then click the three dot menu and select ‘Show original’. You may also need to allow pop ups from mail.google.com





Once you display the headers and body, you will likely see text that is readable, but probably seems nonsensical. You will likely see familiar email addresses and may recognize snippets of the message. You can then copy and paste all of this into the reporting process. Just be conscious that your personal email address and the message details will also be in here as the email recipient, so make sure you're comfortable sending this information. If you're not, you may choose to remove some details from the text - just try to limit your edits. A helpful technique is to replace removed text with a marker like "REDACTED" rather than just deleting it.

You can use this information to put quality reports into NetBeacon, this will help ensure your report is as actionable as possible. You could do this by copying and pasting text, or by taking a screenshot. On an Apple computer, you can press (Shift-Command-5) to take a screenshot, on Windows, you can use the Snipping Tool.

Summary

Phishing is an attempt to trick people into sharing important or sensitive information— for example logins, passwords, credit card numbers or banking information – in either a personal or business context.

A domain name can be involved in a phishing attack. This could be through a **malicious** registration— a domain registered for malicious purposes (i.e., to carry out phishing), or a **compromised** domain name registration is a benign domain name that has been compromised at the website, hosting, email, or DNS level.

A malicious registration is more likely to be suitable for mitigation action at the DNS level. To report phishing to registrars, you can use our free service NetBeacon.

To make an actionable phishing report, it's important you provide sufficient evidence. It's worth learning how to extract the email header and message body. There are great resources available to help you in this process of understanding more about your email client/app.