Shareholder Identification Disclosure - protecting yourself against phishing and employing good cyber security measures

Shareholder Identification Disclosure - protecting yourself against phishing and employing good cyber security measures

As a result of the disclosure element of SRD2 and the sensitive nature of the shareholder identification data, there is a very significant risk of data loss or data theft. For most intermediary firms, this the first time that they will have ever even considered sending such sensitive data via open communications channels. Worryingly, we are hearing that some are not even really considering email communication to be an open channel with all the risk that this entails. So this is a critical point to consider. Email is NOT a secure means of sending confidential data. More on that later.

What is phishing?

Whilst this is not intended to be a comprehensive breakdown of what constitutes phishing, it is important to ensure that there is a baseline understanding of what phishing is and just how damaging it could be in the context of the handling of highly sensitive shareholder data.

The National Cyber Security Centre (NCSC) defines it as "When attackers attempt to trick users into doing 'the wrong thing', such as clicking a bad link that will download malware, or direct them to a dodgy website". As a starting point, this is a useful definition. It serves to provide a simple explanation that conveys the root risk that phishing involves. What it cannot hope to achieve though is to convey the breadth and depth to which attackers can and will go in seeking to convince and deceive their targets. What it also does is risk being too limiting in its simplicity. For example, in the context of SRD2, there need not be any website that a user is directed to. A great deal of damage could be sustained even without actually clicking on any nefarious links. Perhaps therefore, a more helpful way of thinking about phishing is that it is simply misdirection. It is the act of directing your attention away from potential red flags and towards calming, reassuring measures that seek to convince you that the originator of the message is bona fide. In the case of basic attacks, these measures tend to be general in nature and non-specific.

So, if that is the basis of phishing, then what does the worst example of it look like? Well normally, jargon on top of jargon is not particularly helpful. In this case however, there is another term that starts to uncover the real danger of the nefarious practice - Spear Phishing. Instead of a more

broadcast, blanket approach to spamming potentially thousands or millions of recipients, Spear Phishing as it is known is characterised by a next-gen level of sophistication where a great deal more effort has gone in to executing the sender's deception. It might involve directly addressing a member of your staff and trying to convince them of the validity of the request by supplying ancillary elements of information that the phisher has picked up along the way. This can be achieved by means of accessing from the rich pool of public internet information that exists on our businesses and processes as well as much more sophisticated social engineering that might target individual staff, perhaps identified through professional social media profiles.

In the context of SRD2, what if you received an email from Jonathan Fothergill at the oil and gas giant EnerCo in Texas in the US? Both person and company are imaginary to protect the innocent. What if the email made a formal request for disclosure of shareholder information and did so in the format helpfully prescribed by SWIFT in their new MX message structure? What might you do to satisfy yourself that the originator of the request was genuine? Let's consider a non-exhaustive selection of possible means of verification:

Email address

- Does it look valid? Does the name in the email address appear to correspond with the name of the person requesting the shareholder data?
- Does the domain in the email address correspond with the company name of the issuing company? Does it appear to be an enterprise domain or a retail / consumer one?
- Do the email headers stand up to scrutiny? (the techie bits that are normally obscured from your view when you open an email in your email application).

Identity verification

- Have you looked up the requestor's name on the company website? Do they appear to be a valid employee of the firm and in particular, does their position warrant them making such a request? e.g. company secretary or equivalent.
- Do they have a convincing LinkedIn profile?
- Have you phoned them to confirm that their supplied phone number is valid?

Message contents

- Are you addressed by name?

- Spelling and grammar - does it look convincing? Are there any obvious mis-translations that could indicate use of a translation tool?

- Request structure - is the request in the new format as expected? (it is possible that requests will not use this format, but if used, it just serves as another datapoint on which to base your decision about verification).

Of course, checking all the above may not be possible in the 24-hour period permitted for such requests, especially if this is just one of a number of similar requests all made at the same time.

Lastly, and unfortunately, all of the above could be faked or spoofed so there is really no safe way of being sure that any approach received via email is from a valid source…….Wait, what??!!

The bottom line is that the only way to be sure of the provenance of such requests is if they are sent from a trusted identity and one that is known to you in advance. Even then you would have to remain vigilant against spoofed email addresses

(https://en.wikipedia.org/wiki/Email_spoofing)

So, what is the answer?

Interim solution:

If you forward your received requests to Instant Actions, we will run them through our industrial strength verification processes to determine a confidence score. We will fully explain the result of this process and then and only then when the requestor achieves a score that meets the criteria pre-arranged as acceptable will we advise you.

Once the validity of source identity is established you then need a secure method to transmit the data to the issuer or their agent. Even if you know the email address of the original source, email is not a secure channel for such personal and confidential data. Most issuers are not on SWIFT so you can't communicate direct that way. When you sanction release of shareholder identities, Instant Actions sets up a Secure Digital Vault on your behalf. This account belongs to you – Instant Actions has no access to it. You transfer the identities into this Digital Vault, flagged for download by the issuer. The issuer is automatically enrolled to Instant Actions when their identity is checked and is notified that they can download the data through a secure end-to-end encrypted channel to which only you and the issuer have access.

End game:

We believe that the safest way of addressing this problem is for the issuers to be pre-enrolled with Instant Actions and to make their requests via the platform. The pre-registration process would involve us using industrial strength validation processes that are proven to be very resilient against all the tactics that bad actors might employ. We would then only forward valid requests to you for completion.

In either of the above scenarios, you can safely release shareholder data to the Secure Digital Vault and instruct us to release the access credentials to the issuer at the same time.

But how likely is a highly sophisticated phishing attack for the purpose of accessing confidential shareholder data?

Is it likely to occur on a frequent basis? No. It is possible? Yes. It is inevitable? Absolutely! Given the prize of the extremely sensitive nature of the data in question, it is almost inconceivable that just as with all other aspects of the transmission of sensitive data over the internet, shareholder identification data will not be targeted by Phishers. It may be immediately after the regulation goes live or it may be 6 or 12 months down the road. The only questions are when will they strike and who will they strike?

What could the consequence of data loss be?

But if I do everything right and follow all the best practice around information security, I'll be OK right? No, not necessarily! Not if you leave it to chance.

Imagine your document, with identifying references or staff names on - perhaps a member of staff's name and your company name buried in the properties of the document. Perhaps a graphic of the company's logo embedded in the word or xls file. You could employ all best practice in securing that document and getting it to a genuine issuer, only for that issuer to mistakenly email it to an unrelated third party instead of one of their internal contacts. Now that document is out in the wild and it has your company details embedded in it. Not because of a mistake that you made but because of a mistake that the issuer made. But who is to say where the mistake originated? Sadly, blame maybe assigned by association. That is unless you are able to present a bullet-proof defensive explanation. One that explains that:

- It was not possible that you were the cause of the data loss as the only place that you ever place such requests is in the appropriate Secure Digital Vault for that issuer and that the only entity

that would have had access to it would have been the issuer. Once you have deposited the data, it is now being processed by them and becomes their and solely their responsibility to keep it safe.

- You are able to provide an audit trail of this having occurred.
- All your outbound shareholder identification disclosure replies are 'washed' documents - i.e. no identifying marks embedded in the docs.

You need to be able to explain and evidence that you have taken all possible measures to be able to keep that data safe right up until the point that the issuer has retrieved it. Immediately after it has been downloaded by the issuer the data is deleted from the digital vault and you can prove compliance with GDPR. If anything happens to it after that, the issuer is responsible and accountable for it.

That is the robust defence that your information security experts and PR people must be able to present to the journalists when they come looking for their stories or the regulators when they come looking for assurances or worse – an audit.

If this feels a little like an abdication of your responsibility as an account servicer, it is not! You will have done everything in your power to protect your customers' data and you will have adopted all reasonable measures to keep that data safe both in transit and at rest. You will have taken measures that the drafters of the directive and the regulators did not even conceive of. In other words, you will be able to demonstrate that you went above and beyond in your commitment to honour your responsibilities in respect of GDPR as well as good information security principles. If you did all of the above, you will have significantly mitigated if not eliminated this new reputational risk to your business. Should you then subsequently read about SRD2-related client data breaches in the industry press, it is highly likely that those stories will reference your competitors and not you…..

Defence against Phishing: Why a multi-tiered approach is required

Of course, the accepted wisdom is that successful anti-phishing measures involve technology, processes and people. So while there is no silver bullet, getting the technology and the processes right allows you to concentrate on making sure that your staff are well trained in closing down the human element of risk. Ensuring that they are trained to recognise risky communications and that they are completely clear on what is permitted in terms of release of data (including the tools that are permitted) and what is not. Deploying such measures will always be a trade-off between resilience against phishing attacks whilst at the same time minimising disruption and friction in the business.

The NCSC suggests that firms:

1. Make it difficult for attackers to reach users - Control and limit the data that is publicly available that could be used in a phishing attack. This could come from your website or from social media profiles.

2. Help users identify and report suspected phishing emails - Ensure adequate training is provided to frontline staff who might be the target of such attacks and limit their number.

3. Protect organisation from the effects of undetected phishing emails - Seek to make it impossible to copy/paste sensitive data from secure repositories to insecure channels such as email. Put in place security gates that close automatically and require privileged overriding by information security experts.

4. Respond quickly to incidents - Create a culture of freedom to report suspected attacks or suspected breaches and execute on countermeasures quickly.

Q. What is one of the most effective means of avoiding falling prey to such attacks in respect of SRD2?

A. Never, ever respond to such requests via email. Email is simply not a sufficiently secure method of transmission for sensitive data and moreover is actively targeted by phishers. Use encrypted channels only and preferably those using technology such as a Secure Digital Vault.

Q. But these are difficult to setup aren't they?

A. No, Instant Actions can setup everything you need in a matter of days and there is no systems integration required. Feel free to contact us to review the options and see how quickly a robust solution can be put in place for you.

For more information please contact: enquiries@instant-actions.com

Limitations

provided for informational purposes only. The information contained in this document is subject to change without notice and does not constitute any form of warranty, representation, or undertaking. Nothing herein should in any way be deemed to alter the legal rights and obligations contained in agreements between Instant Actions and/or its affiliates and their clients relating to any of the products or services described herein. Nothing herein is intended to constitute legal, tax, accounting or other professional advice. Instant Actions makes no warranties whatsoever, either express or implied, as to merchantability, fitness for a particular purpose, or any other matter. Without limiting the foregoing, Instant Actions makes no representation or warranty that any data or information supplied to or by it are complete or free from errors, omissions, or defects.