CASE STUDY

CATALYST:

ADVANCING DIGITAL AUTHENTICATION

Table of Contents

The Rising Mistrust Towards Your Email

Emails are inherently built into our daily business activities, from contacting customers to sharing fles with colleagues. However, our emails have increasingly become a weak point in any cybersecurity infrastructure.

Mimecast reported that 54% of surveyed organisations saw an increase in phishing email scams from 2018 to 2019.

The infamous email scam by an alleged Nigerian Prince or receivers saw individuals invest their money and time into a phoney investment scandal [2]. Users provided their bank details to a previously unknown email account after being told that money would be transferred to them under the pretence of "safekeeping" the investment funds. This would lead to money being withdrawn from the user's account without their consent. In 2018, it was reported that Americans lost an average of $2,133 in 2018 to these types of frauds [3]. However, this type of scam has evolved from requesting bank details to asking for personal information.

These well-known scams can be difcult to detect as they become more advanced. Often, anti-malware software can detect fraudulent email content and eliminate the email before it can be opened [4]. However, it is estimated that the average user receives +120 emails a day [5], which makes it easy for some email scams to enter an inbox unnoticed.

Identity Issues

Phishing emails are so efective because they deceive the individual into believing they've received an authentic email. It is one instance in which email fraud is accomplished that requires confdential information to be shared. Most often, people can detect the scam because the email address doesn't align with the organisation's website address, there are spelling or grammar errors [6] or there is a non-specifc greeting [7]. The key challenge is determining the identity of the sender [8].

Broadly, a digital identity can be defned as the information about a company or individual that is online [9]. This can be difcult to control when our digital identity can be created via a range from diferent services and platforms in which individuals or companies much relinquish some of their information.

Individuals often must blindly trust that companies have control of their data and securely store it. Most importantly, individuals trust that this data is not shared with unauthorised third parties. Therefore, customers and clients trust that digital communication from companies is genuine. When this isn't achieved, then there becomes a breakdown in trust between companies and clients. As a consequence, 73% of Business Email Compromise (BEC) victims claim that they're sufer direct fnancial loss [1].

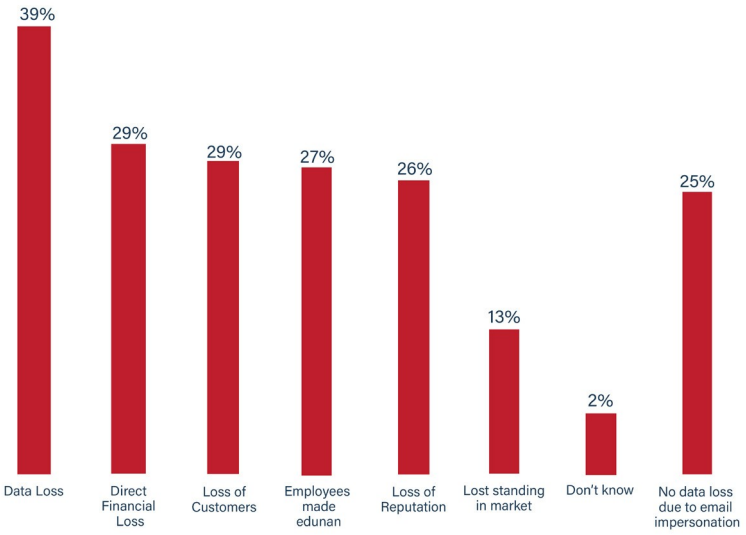


Figure 1. *The impact on businesses after they become victim of an email impersonation case in 2019*

Email impersonation can be difcult for companies to combat as the information that is used against them is often in the public space. Unfortunately, it is often the responsibility of customers to be aware of potential phishing scams. Companies can only promote good practices to their consumers by emphasising awareness, advertising anti-malware software or includes partial confdential information in the content to authenticate the email.

The impersonation of emails for companies can also imply that they are at risk of other cybersecurity issues. A scam email for a customer can often be disregarded due to the frequency of them but, if the email appears to come from an authentic email address then it can allude to a data breach. In addition, should the consumer open the fraudulent email, there is the possibility of malware being introduced into their local hardware.

Blockchain Technology

Blockchain and Distributed Ledger Technology (DLT) ofers unique unforgeable digital signatures that can eliminate the engagement by unsuspecting clients with impersonation emails. This technology ofers companies the opportunity to integrate a trustless method of providing a company employee's digital identity using the immutable and cryptographic components of DLT.

Catalyst is Red Skies native DLT platform that has been created to specifcally streamline workfow processes to reduce administrative tasks and increase productivity. For email security and data transfer, Catalyst ofers an alternative for proving digital identity in emails.

Authentication – Each member of an organisation is often assigned their own email account, which can be hacked via phishing scams or malware integrated into email content. Once hacked, the trust in that email account will be reduced. Using digital signatures, Catalyst can ofer a trustless system for an organisation's email accounts.

Immutability – The traceability of emails can be difcult with so many being sent and received every day. Using Catalyst, each email sent internally can be automatically timestamped on the blockchain to ensure each email is sent.

Verifcation – Business email accounts can often be identifed by the username followed by the "@" symbol and domain component. However, this can often be forged or given a negligible change to appear trustworthy. Catalyst ofers an additional proof of identity using cryptographic digital signatures uniquely assigned to each individual.

The time-consuming nature of email attacks can be exhausting and reduce productivity levels across an organisation. With 88% of organisations experiencing email-based spoofng of business partners and vendors in 2019[1] it is clear that the solution of anti-malware software doesn't completely solve the issue.

The challenge is to ensure that each individual can verify the digital identity of an employee to ensure that the email account is not compromised. With this in mind, it is time that companies look to new technologies that ofer tamperproof and verifable solutions.

Using Catalyst and Timescribe together, a solution can be found that creates unique and unforgeable digital signatures, as well as an immutable record of all emails sent by the organisation For a company, this can ensure that internal emails verifable and trustworthy and external impersonation emails can be challenged immediately. Emails can become more secure, trustworthy and there can be a reduction in time for manually checking of email authentication.

Red Skies products and services help companies, organisations and individuals streamline their workfow to ensure time is spent on the important tasks to increase productivity using blockchain-based solutions. For more information about the company, then visit our website.

Improving Email Authentication

Emails can contain highly confdential or sensitive information that shouldn't be available to unrelated parties. Companies that communicate with clients via email need to be able to authenticate their identity and reassure that users' confdential information remains secure.

Timescribe is the frst product released by Red Skies that ofers timestamping functionality with blockchain advantages. The product uses blockchain to create a unique hash of email email can be stored on or of chain. Timescribe uses the cryptographic component of blockchain to create a distinctive digital signature that signs each email. A digital signature ofers the ability to link each timestamp to a specifc individual.

Blockchain ofers the functionality of creating proofs of emails sent by companies that can be authenticated for all receivers. This reduces the time taken to manually verify that emails are authenticate.

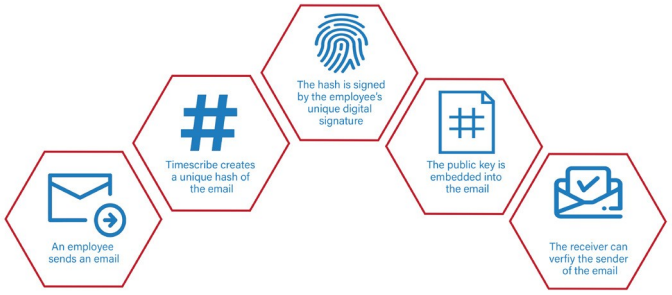


Figure 2. *An email authentication system that utilises the cryptographic component of blockchain technologies to create unique tamperproof digital signatures to sign emails.*

This alternative solution ofers a plug-in of Timescribe that ofers full automation for companies (fgure 2). Companies would be required to sign up to an Red Skies portal that would include a Know Your Customer (KYC) process to ensure company validity. The company's email application will receive a plug-in that would automatically generate a timestamp uniquely signed with the company's digital signature for all emails sent from a company domain. This would require the portal to check the "sender domain", rather than the "from domain", to reduce the likelihood of potential impersonation occurring. The receiver would then be able to verify the email's authenticity by comparing the digital signature with the company's known one via the portal.

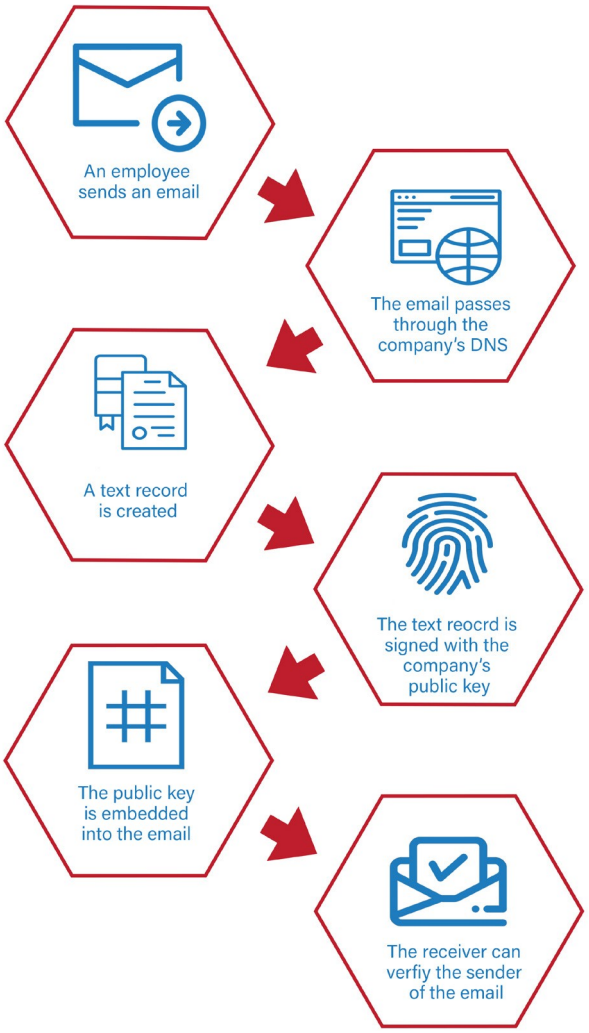
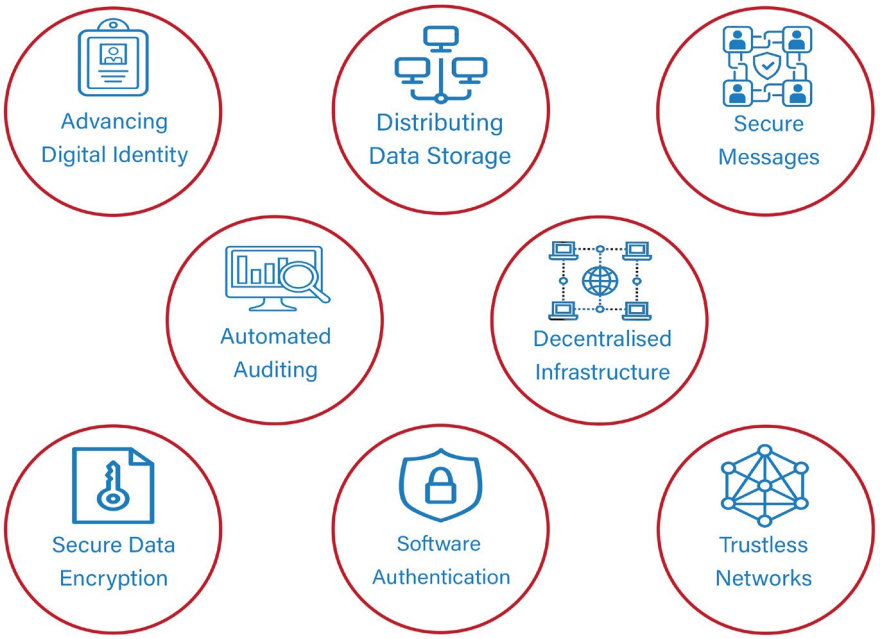


Figure 3. *An email authentication system that utilises the DNS for automation of digital signatures to be added to all emails sent from a company with their public key attached.*

Another solution can ofer additional responsibility for the organisation for their own cybersecurity measures. The email sent would automatically travel through the Domain Name System (DNS) and that will create a text record that is linked to a unique blockchain public key (fgure 3). This would be automatically added to the bottom of the email. The external individual would then be able to verify the email by checking that the public key is in fact the one associated with the company. This solution ofers the opportunity for companies to gain control of their DNS and ensure their authenticity for their clients and users.

Figure 4. *The future of cybersecurity solutions leveraging blockchain technologies. Catalyst, by Red Skies, ofers immutability, scalability, security and speed for all solutions listed below.*



Advancing Current Solutions

Email fraud is often countered with a combination of threat protection (i.e. anti-malware software), advocated awareness and an adaptable and fexible strategy in the event of an attack. The various components of this strategy can be time consuming and require a lot of efort to upkeep.

Blockchain enables an automation and implementation of a trustworthy solution against the impersonation of a digital identity. The technology doesn't require raising additional awareness or having to create a response strategy to the potential problem because of its tamperproof nature.

Blockchain technologies can construct a chronological path of data owned by a specifc company or group of individuals. Asymmetric key cryptography is used to create a public-private key pair. The public key can be shared with external individuals; this public key allows verifcation of any messages or transactions digitally signed by the private key belonging to the owner of the key pair. These signatures are created in such a way that only the owner of the private key could have possibly created this signature that is verifable with the corresponding public key.

Automation – Timescribe fawlessly integrates into your current email provider application to provide a method of verifable digital identity.

Building Trust – Timescribe reduces the risk of impersonated emails being sent and opened by clients as they can quickly verify each email against the company's public key.

Immutability – Blockchain technologies use cryptography to link data in a chronological order. This make the verifed data tamperproof, even if it's stored of chain.

Secure – The record of emails sent from a company will be kept in a tamperproof manner by leveraging blockchain technologies.

Improving Email Security

Implementing an efective email security strategy can be difcult for companies that send hundreds or thousands of emails every day. Tracking impersonating emails sent to clients and customers cannot often be achieved due to resource constraints.

With the rise of social media and the public availability of information has led to an increased in email frauds and scams. Consequently, the probability of success for more advanced tactics of email fraud is 75.5% [11] Organisations need to ensure that their digital communication and their customers' personal data remains secure.

Domain-based Message Authentication Reporting and Conference (DMARC) ofers an authentication system for digital communication [12] For domain owners, they are able to register their domain for email authentication and ensure policy for messages that fail authentication. For email receivers, they can trust that the email domain has been authenticated by a third-party.

Blockchain technologies ofer trustless and secure authentication that can be integrated into cybersecurity strategies. A solution using Catalyst and Timescribe can ofer true authentication by companies undergoing a third-party KYC process before receiving an unforgeable private-public key pair. For consumers, this can provide peace of mind as the information cannot be altered by any party and restore trust in digital communication.

67%
of organisations said email impersonation scams increased between 2018 and 2019[1]

"...extending full digital ID coverage could unlock economic value equivalent to 3 to 13 percent of GDP in 2030."
- McKinsey & Company [17]

The Future of Protecting Digital Identities

With the increasing automation and digitalisation of services, the importance of secure digital identities is increasing. The ability to have digital identifcation and authentication that can be audited or authenticated is crucial [13]

For businesses, they can provide authenticated and secure digital communication with clients and customers. Consequently, any data or information transferred can be categorised as trustworthy too.

For individuals, the creation and protection of their digital identity aids their participation in their social, economic and political life. The authentication of a digital identity provides the ability for global sustainable development. UNICEF recognised that in India only 61% of wage payments reach eligible workers due to a lack of digital identity management and authentication in labour processes [14] This is because of inadequate digital identity management systems.

As digital identities to continue to develop and grow, there is the expectation that public supervision for digital identifcation will be demanded [15] Blockchain technologies enable a trustless method of digital identity authentication.

Conclusion

With the prevalence of email impersonation, companies need to provide a method of authentication for their digital communication with clients and customers. This is required to establish and maintain a high-level of trust.

The challenge is to ensure that a high level of assurance can be provided for clients and customers. Blockchain technologies can provide a high-level automated authentication method using cryptography.

The automation of this system can ensure the reduction in risk of email impersonation leading to fnancial losses. In addition, the ability to verify the digital identity on digital communication can reduce the spread of malware or misinformation.

The addition of an authentication system can raise the alarm of a fraudulent email by a customer faster, reducing and minimising damage. The solution provides companies the opportunity to highlight that they are capable of minimising cybersecurity risks and highlights their proactive actions towards reducing risks.

The trustless nature of blockchain technology prevents tampering and impersonation of a digital identity. The immutable component of Timescribe ofers a chronological record of emails sent from the authenticated company. This method of authentication can be trusted by all parties.

Blockchain technology puts companies at the forefront of transforming and protecting their digital identity. The technology enables privacy, security, equality and the ability to continue building new opportunities with clients and customers.

16

Our team ofers blockchain training, strategic advisory, development services and opportunities for joint ventures and co-creation. We're here to help you and your organisation along your blockchain journey.

References

1 https://www.mimecast.com/the-state-of-email-security-2019/download-hub/

2 https://www.popsci.com/story/technology/nigerian-prince-scam-social-engineering/

3 https://www.cnbc.com/2019/04/18/nigerian-prince-scams-still-rake-in-over-700000-dollars-a-year.html

4 https://www.getsafeonline.org/online-safety-and-security/ceo-impersonation-fraud/

5 https://www.ncsc.gov.uk/guidance/whaling-how-it-works-and-what-your-organisation-can-do-about-it

6 https://books.google.co.uk/books?id=dcOWDwAAQBAJ&pg=PA111&lpg=PA111&dq=willems+2019+malicious+software&source=bl&ots=F1PSmUxkpp&sig=ACfU3U2IjLQfrTCHW53OFQ2P5jF_0qK0JQ&hl=en&sa=X&ved=2ahUKEwi01vjT-PHpAhWSgVwKHYwmD44Q6AEwAHoECAoQAQ#v=onepage&q=willems%202019%20malicious%20software&f=false

7 https://hbr.org/2019/01/how-to-spend-way-less-time-on-email-every-day

8 https://frsecure.com/blog/is-that-sender-for-real-three-ways-to-verify-the-identity-of-an-email/

9 https://www.actionfraud.police.uk/scam-emails

10 https://www.adt.com/resources/prevent-phishing

11 https://www.fnextra.com/blogposting/18850/fraud-in-fnance-who-can-defend-our-digital-identity

12 https://www.lawyersmutualnc.com/blog/6-ways-to-defend-against-email-impersonation-attacks

13 https://www.mimecast.com/globalassets/cyber-resilience-content/the_state_of_email_security_report_2020.pdf

14 https://dmarc.org/

15 https://secureidentityalliance.org/publications-docman/public/4-july-2016-report-digital-identity/fle

16 https://www.gsma.com/identity/key-facts-stats

17 https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/identity/digital-identity-services/trends

18 https://www.futureagenda.org/focus-on/future-of-digital-identity/

19 https://www.mckinsey.com/~/media/mckinsey/featured%20insights/innovation/the%20value%20of%20digital%20id%20for%20the%20global%20economy%20and%20society/digital-id-a-key-to-inclusive-growth-january%202019.ashx


AT&T
59%
Touch ID or Enter Passcode
1
2 ABC
3 DEF
4 GHI
5 JKL
6 MNO
7 PQRS
8 TUV
9 WXYZ
0
Emergency
Cancel