EVIDEN

Building Resilience

Tech Solutions Against Phishing

Management Summary

Phishing attacks have become one of the most dominant and rapidly growing cybercrimes in recent years. These malicious attempts involve deceiving IT users into revealing sensitive information, typically through deceptive emails or messages leading to fraudulent websites. Several high-profile incidents, such as the SolarWinds breach[1] and the Colonial Pipeline hack[2] have exposed the severity of the issue. Phishing has evolved into a sophisticated threat, and the use of Artificial Intelligence has made it even more challenging to combat. Phishing attacks typically involve an attacker sending a deceptive message with a counterfeit link, often mimicking well-known providers or colleagues.

Phishing incidents have surged, with over 500 million attacks reported in 2022[3] , and a 61% increase in attacks between May and October 2022[4] . Notably, the USA saw around 300,497 phishing victims in 2022. Several laws in France, Germany and other countries implicitly require phishing protection to combat this threat. While secure passwords, one-time passwords (OTP), biometric authentication, and CAPTCHAs enhance security, they do not prevent phishing attacks. Certificate-based authentication, supported by a Public Key Infrastructure (PKI), is an effective countermeasure against phishing. This technology helps to verify the authenticity of the client‘s public signature key, making phishing attempts much more challenging.

Instead of a PKI and digital certificates, the Fast Identity Online (FIDO) authentication infrastructure can be used to authenticate the client’s public signature key used for phishing protection. This alternative is especially attractive if no PKI is available. Both certificate-based and FIDO authentication become even more secure if token binding is employed. End-to-end cryptographic email protection, including the use of encryption and digital signatures, is another important technology that protects against phishing. It enhances email security and makes it difficult for attackers to impersonate legitimate senders.

Eviden offers a range of powerful security solutions to prevent phishing attacks, including certificate-based authentication and FIDO authentication with token binding, as well as cryptographic email protection. The most important of these solutions are the CardOS operating system, IDnomic PKI (including a cloud-based PKI-as-a-service offering), and cryptovision GreenShield. Organizations are encouraged to contact Eviden to discuss their specific needs.

1. https://www.techtarget.com/whatis/feature/SolarWinds-hack-explained-Everything-you-need-to-know
2. https://www.techtarget.com/whatis/feature/Colonial-Pipeline-hack-explained-Everything-you-need-to-know
3. https://www.forbes.com/advisor/business/phishing-statistics/
4. tinyurl.com/mryn2zz9

Table of content

Introduction 4
Phishing as an increasing threat scenario 6
- Phishing explained 6
- Statistics and trends 6
- Phishing methods 7
- Techniques that don't help against phishing 7

Legal frameworks to combat phishing 8
Certificate-based authentication as a countermeasure 8
- Signature-based authentication 9
- Certificate-based authentication 9
- Public Key Infrastructure (PKI) 9

FIDO authentication as a countermeasure 9
- FIDO authentication 9
- FIDO infrastructure 10

End-to-end message protection as a countermeasure 10
- End-to-end cryptographic protection 10
- How email signatures and encryption protect from phishing 10
- Deployment 10

Eviden Digital Identity solutions 11
- Certificate-Based Authentication by Eviden 11
- FIDO authentication by Eviden 12
- Cryptographic email protection by Eviden 12
- Eviden references 12

Why investing in phishing-resilient technologies is critical 13
Conclusion 13

Introduction

Phishing attacks are malicious attempts to deceive IT users into revealing login credentials or other sensitive information. They typically involve deceptive emails or messages that lead recipients to fraudulent websites. In recent years, the digital landscape has witnessed an alarming surge in phishing attacks, making it one of today's most dominant and fastest-growing cybercrimes

Numerous examples of phishing-based security breaches have been covered in the media (see adjacent boxes).

Phishing-based security breaches

Here are some of the most devastating phishing-based security breaches:

SolarWinds: The SolarWinds security breach, discovered in December 2020, was a sophisticated cyberattack that affected various U.S. government agencies and private sector organizations. It involved hackers inserting malicious code into a software update for SolarWinds' Orion platform, a widely used network monitoring tool. When customers installed this compromised update, it allowed the attackers to gain unauthorized access to their networks. The attack started with an account being hacked. From this initial foothold, the attackers were able to send out phishing emails to get victims to click on a link that would deploy a backdoor Trojan. The monetary damage of the SolarWinds security breach has been estimated to be around $90 million.[5]

Colonial Pipeline: The Colonial Pipeline hack occurred in May 2021 and involved a ransomware attack on one of the largest fuel pipelines in the United States. The attackers encrypted the pipeline's data and successfully demanded a ransom in exchange for the decryption key. Again, the hack started with a phishing attack.[6]

U.S. state health agency: In February 2022, the sensitive medical data of more than 1,200 U.S. residents was exposed after a successful phishing attack against a health agency in Washington State.[7]

NFT Investments: In January 2023, NFT Investments, an incubator specializing in NFT technology, became victim of a phishing attack from an unknown external source. The attack resulted in the loss of $250,000. [8]

Ludwigsburg district: In May 2023, cyber criminals attacked the Ludwigsburg district administration in Germany. Consequently, the district office had to be closed and completely shut down. [9]

Microsoft: In October 2023, a new phishing campaign targeted Microsoft 365 accounts in the USA. Targets of this phishing campaign were executives and high-ranking employees from various industries. [10]

Attack on the Irish Health Service Executive (2021)

In 2021, the Health Service Executive (HSE) of Ireland suffered a major ransomware cyberattack, which caused all its IT systems nationwide to be shut down during the Covid pandemy[11]. It was the largest known security breach at a health service IT system in history. The attack was carried out by a Russian criminal gang known as Wizard Spider.

The cyber attack began on 18 March 2021 with a malware infecting an HSE workstation. This infection was possible because the user of this workstation opened a malicious Microsoft Excel file that was included in a phishing email. After gaining unauthorized access to the HSE's IT environment, the attacker moved across the network over a period of eight weeks. He compromised privileged accounts, infected numerous servers, and began exfiltrating data. In addition, he extended the attack to other systems, including the IT environments of HSE-affiliated hospitals.

For weeks, the HSE's IT administrators failed to act on several warning signs that a massive attack was imminent. The incident was only detected when the Conti ransomware became active on 14 May 2021 and caused widespread IT disruption by encrypting data. The attack resulted in an almost complete shutdown of the HSE's national and local networks and disruption of service at several clinics and health services. Appointments were down by 80%.

The Conti Group initially demanded a $20 million ransom in cryptocurrency in exchange for the digital key to decrypt the compromised HSE servers. After the case had become public and there was an outcry from the public, the Conti gang gave the HSE the decryption keys for free. The costs for the recovery is estimated at around 530 million Euros. Medical information for at least 520 patients, as well as corporate documents were published online.

5. https://www.techtarget.com/whatis/feature/SolarWinds-hack-explained-Everything-you-need-to-know
6. https://www.techtarget.com/whatis/feature/Colonial-Pipeline-hack-explained-Everything-you-need-to-know
7. https://portswigger.net/daily-swig/washington-residents-medical-data-exposed-by-phishing-attack-on-spokane-regional-health-district
8. https://www.proactiveinvestors.co.uk/companies/news/1003057/nft-investments-hit-by-us-250-000-phishing-attack-implements-incident-response-plan-1003057.html
9. https://www.heise.de/news/Cyber-Vorfaelle-beim-Verband-der-Pharmaindustrie-Kreis-Ludwigsburg-und-Sysco-9018251.html
10. https://www.bleepingcomputer.com/news/security/evilproxy-uses-indeedcom-open-redirect-for-microsoft-365-phishing/
11. https://www.hse.ie/eng/services/publications/conti-cyber-attack-on-the-hse-full-report.pdf

This whitepaper aims to provide a comprehensive overview of phishing attacks and effective solutions to combat them. As will be shown, Eviden Digital Identity offers a comprehensive suite of advanced products to bolster phishing resilience

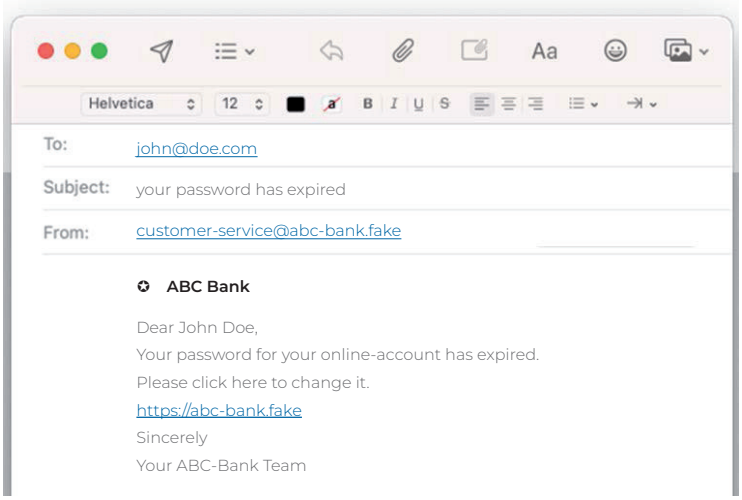


Figure 1: A phishing attack starts with the attacker sending a deceptive message containing a counterfeit link. This is typically done by email or messenger

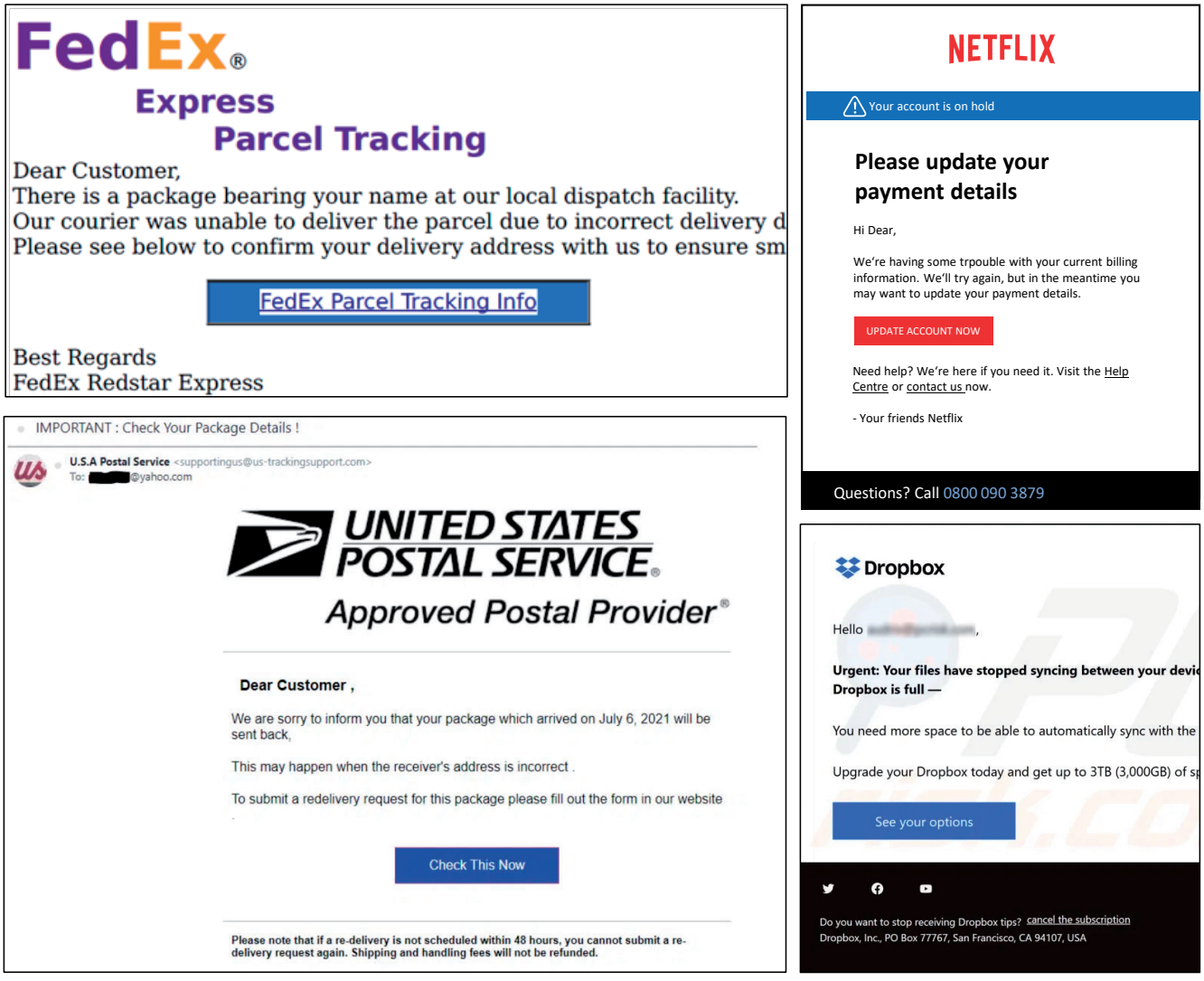


Figure 2: Many phishing emails look like they come from well-known companies.

Phishing as an increasing threat scenario

Phishing explained

A phishing attack typically involves the following steps:

1. The attacker sends a fake message containing a counterfeit link to the victim. This is typically done by email or messenger (see Figures 1 and 2).
2. The victim unwittingly follows the link, leading to a fake server (e.g., a fraudulent website).
3. The fake server prompts the victim to input authentication information, such as a password.
4. The victim, unaware of the ruse, enters their password.
5. The fake server then uses the obtained password to access the victim's account on the authentic server.

The probability of success increases if the email looks as if it comes from a well-known provider or work colleague. As phishing involves the attacker manipulating messages exchanged between two parties, phishing belongs to the family of man-in-the-middle attacks.

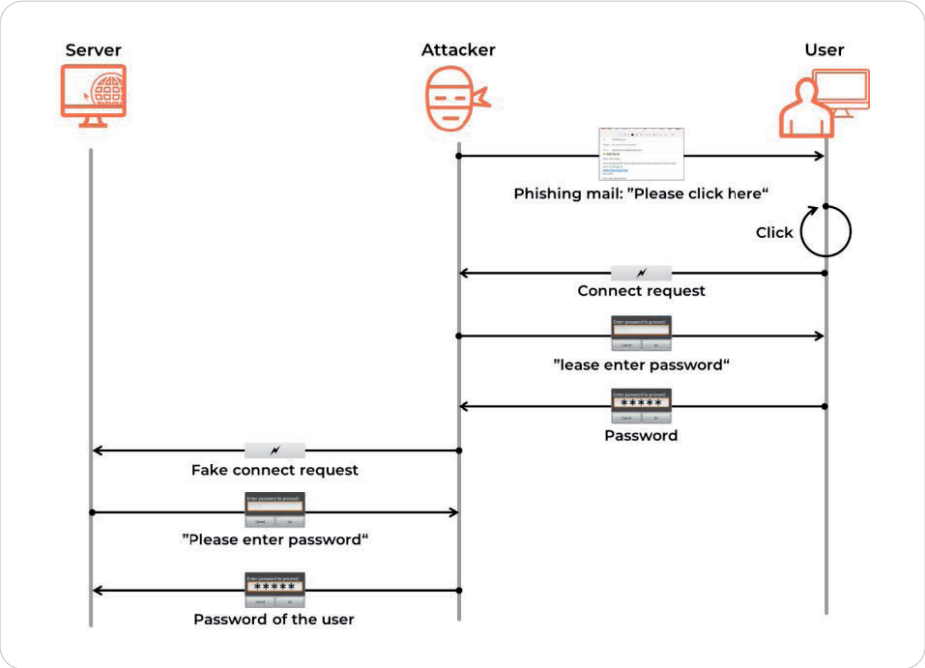


Figure 3: Phishing involves manipulating messages exchanged between two parties. It represents a man-in-the-middle attack

Statistics and trends

Phishing, a technique known since the 1990s, has caused substantial damage with over 500 million attacks reported in 2022 alone, according to Forbes[12]. CNBC also reports a 61% increase in phishing attacks between May and October 2022 compared to the previous year[13]. Notably, the USA saw around 300,497 phishing victims in 2022.

As highlighted by reputable sources such as DIGIT NEWS ("Phishing the Most Dominant and Fastest Growing Internet Crime of 2023")[14] , CNBC ("Phishing attacks are increasing and getting more sophisticated")[15] , and Infosecurity Magazine ("Phishing – The 2023 Cybersecurity Threat")[16] , phishing attacks have become increasingly sophisticated and pose a substantial threat to organizations worldwide.

Lately, Artificial Intelligence (AI) has become an important means to prepare and carry out phishing attacks. An attacker can use AI tools to create hundreds of thousands of tailor-made phishing mails and fake websites within a short time period. Current AI systems are capable of producing grammatically correct texts in dozens of languages that are hard for both spam filters and the average individual to catch. In the near future, voice and face cloning are expected to become instrumental in phishing attacks, too.

All in all, phishing poses a significant threat to organizations, leading to financial losses, data breaches, and reputational damage.

12. https://www.forbes.com/advisor/business/phishing-statistics/
13. tinyurl.com/mryn2zz9
14. https://www.digit.fyi/phishing-the-most-dominant-and-fastest-growing-internet-crime-of-2023
15. https://www.cnbc.com/2023/01/07/phishing-attacks-are-increasing-and-getting-more-sophisticated.html
16. tinyurl.com/5emb7yny

Phishing methods

Various phishing variants exist, including the following:

- Spear-phishing: Spear-phishing is a targeted form of phishing where cyber attackers customize their deceptive messages to appear highly relevant to specific individuals or organizations. It often involves thorough research on the intended victims.
- Vishing: Vishing, or voice phishing, is a technique where the attacker uses phone calls or voice messages to trick the victim into revealing sensitive information or taking certain actions. Typically, vishing scams involve impersonating legitimate organizations, such as banks or government agencies.
- Smishing: Smishing, or SMS phishing, is a cyberattack technique where the attacker uses text messages to deceive individuals into divulging sensitive information or clicking on malicious links. These deceptive messages often impersonate trusted sources, like banks or government agencies.

Many more variants are mentioned in the literature. A treatise of these is beyond the scope of this paper.

Techniques that don’t help against phishing

Authentication is a fundamental concept in IT security. It refers to the process of verifying the identity of a user, device, or system attempting to access a specific resource. This verification is typically achieved through the presentation of a password, a smart card, or biometric data. Authentication serves as the first line of defense against unauthorized access.

It is important to note that there are several techniques that make authentication processes more secure but don’t prevent phishing. Some of these are listed in the following:

- Secure passwords: Passwords that are hard to guess, while being important, don’t protect against phishing, as a phishing attack doesn‘t involve password guessing.
- One-Time Passwords (OTP) and SMS codes: These techniques are prone to man-in-the-middle attacks and interception by malicious actors, too. Nevertheless, OTPs, generated on a smart card can be a part of an anti-phishing strategy.
- Biometric authentication against the server: Biometric methods are not immune to man-in-the-middle attacks. However, biometric authentication against the smart card can be a part of an anti-phishing strategy.
- CAPTCHAs: A CAPTCHA, while helpful to prevent denial-of-service attacks, does not address the problem of man-in-the-middle attacks.

Legal frameworks to combat phishing

It is known from experience that it is not enough to merely recommend that companies and authorities implement IT security measures. Instead, legal regulations are needed that explicitly require this & impose penalties for non-compliance.

Legal regulations relevant for phishing already exist in many countries. One example is the Network and Information Security Directive (NIS2) of the European Union, which affects companies and public authorities with 50 or more employees and annual sales of ten million euros or more. Among other things, NIS2[17] introduces personal liability for managing directors and board members, who will face hefty fines for breaches of cybersecurity obligations. Phishing resilience, while not mentioned literally, is regarded an indispensable means to fulfill the requirements of NIS2. The same is true for the EU General Data Protection Regulation (GDPR).

In France, the LPM (Loi de Programmation Militaire), a piece of legislation that outlines the country's defense strategy, military capabilities, and budget allocation for a specified period, requires phishing protection implicitly.

In Germany, several laws require the use of phishing protection implicitly:

- Verschlusssachenanweisung: This German Regulation for authorities and suppliers can only be fulfilled if phishing-protection measures are implemented.[18]
- BSI KritisV directive: The same is true for this directive targeting the security of critical infrastrutures.[19]
- IT-Sicherheitsgesetz 2.0: This act to increase the security of information-technology systems implicitely requires phishing protection, too.[20]

In the U.S., a Whitehouse directive signed by President Joe Biden on May 12th, 2021, requires phishing-resiliant authentication for U.S. agencies.[21] It states: "Agency systems must discontinue support for authentication methods that fail to resist phishing, such as protocols that register phone numbers for SMS or voice calls, supply one-time codes, or receive push notifications." Migration is required within 180 days. Those who cannot meet the November 8th deadline are required to provide reports every 60 days until they have fully deployed phishing-resiliant authentication.

As phishing is a worldwide phenomenon, there is a need for international collaboration in defending against it. Businesses have a responsibility to prevent phishing to protect customers, employees, their reputation, and financial stability. To fulfill this responsibility, companies should invest in cybersecurity and take proactive measures to combat phishing attacks.

Certificate-based authentication as a countermeasure

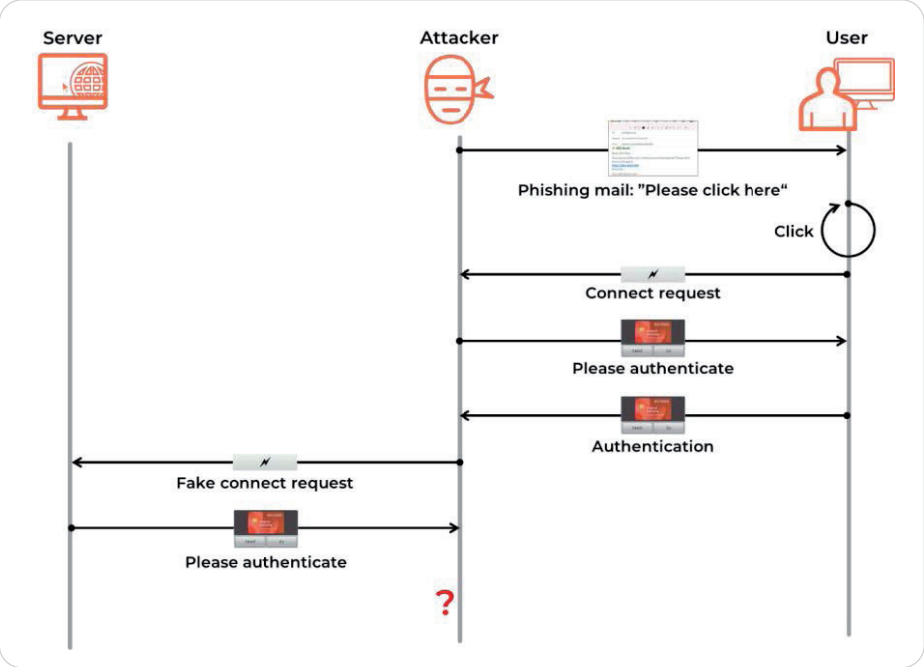


Figure 4: Signature-based authentication is a challenge-response mechanism that combats phishing attacks

17. https://tinyurl.com/mr4cxmyd, https://tinyurl.com/5eath8fm
18. https://tinyurl.com/yc7fre76
19. https://www.gesetze-im-internet.de/bsi-kritisv/
20. https://www.bsi.bund.de/DE/Das-BSI/Auftrag/Gesetze-und-Verordnungen/IT-SiG/2-0/it_sig-2-0_node.html
21. https://www.yubico.com/blog/a-new-white-house-directive-phishing-resistance/

Signature-based authentication

Authentication based on digital signatures is an important countermeasure against phishing. Typically, a challenge-response-authentication protocol like the following is carried out:

- The server sends a challenge to the client. The challenge includes a random number, the current time, and the URL of the server.
- The client signs the challenge and sends it back to the server as the response.
- The server verifies the signature. If it is correct & if the challenge is unchanged, the authentication is successful.

Certificate-based authentication

Signature-based authentication requires that the server knows the public signature key of the client. Of course, this can be achieved by the client sending its public signature key with the response, but in this case the public key might not be authentic. The most obvious way to establish the authenticity of the key is to use digital certificates. In this case, the authentication protocol works as follows:

1. The server sends a challenge (including a random number, the current time, and the URL of the server) to the server.
2. The client signs the challenge and sends it back to the server as the response. In addition, it sends its digital certificate, which includes its public key.
3. The server verifies the signature and the digital certificate. If everything is correct, the authentication is successful.

Certificate based authentication is phishing-resiliant because the response includes the signed URL of the server. In case of a phishing attack, the URL of the attacking server is signed. If the attacker doesn't change this URL, the server will not accept the response, as it contains a wrong URL. If the attacker does change the URL, the server will not accept the response because the signature is wrong.

To improve security, the technique of token binding can be used.[22] This means that the client not only signs a challenge but also a data set (token) that contains its identity and potentially other information such as a URL. A token can be used over multiple protocol sessions. For an attacker, it is virtually impossible to fake a token and it is useless to steal one, as the identity information contained refers to a different instance and can't be changed.

Public Key Infrastructure (PKI)

Certificate-based authentication requires the existence of an infrastructure that enables the issuing and distribution of digital certificates. In other words, a Public Key Infrastructure (PKI) is necessary. In many cases, an existing corporate PKI can be used. If this is not the case, a public Certification Authority (CA) or a PKI-as-a-service offering can be employed. It is also possible to build a new PKI and use it for certificate-based authentication as well as for other applications.

Public Key Infrastructures represent a proven security technology that protects from many different attacks. They have been effective for more than 25 years. Using a PKI for certificate-based authentication is a widespread and trusted method. Applying this technology in the field of phishing resilience is therefore a logical step that is based on well-understood mechanisms. The use of qualified digital signatures and email encryption can further improve the protection against phishing provided by a PKI

FIDO authentication as a countermeasure

Instead of a PKI, the FIDO-authentication infrastructure can be used for authenticating the public signature key of the client. FIDO, which stands for „Fast Identity Online," is an open industry association and a set of standards and protocols designed to enhance online authentication. FIDO Alliance, the organization behind FIDO, was formed to address the growing challenges associated with traditional password-based authentication methods, which are often vulnerable to various forms of cyberattacks, including phishing

FIDO authentication

The FIDO authentication methods allow each user to generate their own key pair for every server they use. Based on this key pair, signature-based authentication is applied, as introduced above. While less secure than digital certificates, the FIDO method is easier to use in environments that don't include a PKI. However, contrary to a PKI, the used of FIDO authentication can't be extended to digital signatures, encryption and various other authentication use-cases, including VPN access.

Again, the reason why this scheme is phishing resiliant is that the URL of the server is a part of the signed message. Token binding, which further enhances security, can be used, too.

22. https://datatracker.ietf.org/doc/rfc8471/

FIDO infrastructure

FIDO authentication is a mature technology that is used in various contexts across the digital landscape, including online services, websites, financial services, enterprise authentication, government services, healthcare, cloud services, education, IoT devices, mobile apps, and cross-platform authentication.

The adoption of FIDO authentication continues to grow as organizations recognize its benefits in terms of security, user experience, and privacy protection. Users can take advantage of FIDO-compatible devices and authentication methods to improve the security of their online accounts and transactions.

End-to-end message protection as a countermeasure

Making the authentication process more secure with digital signatures is not the only approach to protect from phishing. It is also helpful to prevent phishing emails

End-to-end cryptographic protection

To protect an email from unauthorized reading, it is advisable to use encryption. Modern encryption is based on asymmetric cryptography with algorithms such as RSA and Diffie-Hellman. If in addition protection from tampering and forging email is necessary, digital signatures should be employed. Digital signatures are based on asymmetric cryptography, too. Encryption and digital signatures are similar techniques that can easily be deployed and used together.

To secure emails through cryptography effectively, the recommended approach is to employ end-to-end encryption and signatures. This entails performing encryption, signing, decryption, and verification directly on the user's computer.

Cryptographic email protection in an enterprise should be used with the support of a PKI. While it is also possible to use out-of-band key distribution, this is only advisably in a small user group. Of course, the same PKI can be used for email protection and certificate-based authentication. Certificates can be provided by an internal PKI or a third-party service offered, for example, by a public Certification Authority or a PKI-as-a-service offering, which may be cloud-based.

How email signatures and encryption protect from phishing

Digital signatures provide good protection against phishing emails. If legitimate emails are routinely signed, a user will immediately realize that an unsigned email is suspicious.

Encrypting emails is useful for phishing resilience, too, as an attacker needs to use the recipient's public key to fake a credible mail. While this is possible, it requires an additional step to prepare a phishing email, which makes phishing more difficult. In addition, identical phishing mails sent to thousands of recipients don't work in such a case.

All in all, signing and encrypting increase email security in numerous ways. Protection against phishing is only one of the many benefits this technology provides

Deployment

The deployment of cryptographic email protection is a system integration project. For the management of digital certificates, In many cases an existing PKI can be used. In addition, there are numerous vendors offering PKI services, including cloud-based and PKI-as-a-service solutions. Email encryption and signing has been in use in numerous organizations worldwide for over 20 years. It is a well-established technology, the scope of which goes far beyond phishing prevention. In the near future, PKIs will need to be equipped with post-quantum crypto algorithms to make them resilient against quantum-computer attacks.

Eviden Digital Identity solutions

Eviden brings together its digital, cloud and big data & security business lines. It ia a global leader in data-driven, trusted and sustainable digital transformation. A next-generation digital business, Eviden stems from worldwide leading positions in digital, cloud, data, advanced computing and security.

Eviden Digital Identity is the home of cryptovision, CardOS and IDnomic solutions, developed to protect electronic identities with cryptographic solutions and applications.

Eviden Digital Identity provides several powerful solutions that prevent phishing attacks. In addition, the Eviden portfolio includes products that implement one-time passwords, including CardOS SmartOTP and HOTP/TOTP. However, these solutions are not relevant for phishing resilience

Certificate-Based Authentication by Eviden

Eviden Digital Identity provides a portfolio of solutions that enable the use of certificate-based authentication:

- CardOS: This smart card operating system supports both FIDO and certificate-based authentication.
- cryptovision ePasslet Suite: The cryptovision ePasslet Suite is a Java Card-based framework for smart cards that supports FIDO-token and certificate-based authentication.
- cryptovision SCinterface: This solution represents a platform-agnostic middleware for smart card and token usage. It includes optional extensions for usability and user satisfaction, including VirtualSmatCard and RemoteSmartCard. It supports Certificate Based Authentication, digital signatures, and encryption.
- IDnomic PKI: IDnomic PKI is a robust and powerful multi-tenant Certification Authority solution. It can be used, among other things, to operate a PKI for certificate-based authentication and email protection.
- IDnomic CMS: IDnomic's Credential Management System (CMS) improves the management of digital certificates in a PKI and facilitates the global administration of cryptographic media. Among the PKI applications supported are certificate-based authentication and email protection.
- IDnomic CLM: This Certificate Lifecycle Management (CLM) solution supports a number of helpful functions that makes using a PKI easier, especially in heterogeneous environments. Certificate-based authentication and email protection can profit from this.
- IDnomic Sign: IDnomic Sign enables secure digital signatures that can be used, among other things, for phishing protection.
- Evidian Web Access Manager: The Evidian Web Access Manager includes a reverse-proxy that enables centralized authentication. It offers a range of strong authentication methods, including certificate-based authentication and FIDO with token binding. Once authenticated, users are granted access only to resources for which they have appropriate permissions, helping to safeguard against phishing attempts and unauthorized access.

Figure 5: The CardOS smart card operating system supports both FIDO and certificate-based authentication.

FIDO authentication by Eviden

The following Eviden products support FIDO authentication:

- **CardOS:** The CardOS smart card operating system supports both FIDO-token and certificate-based authentication (the latter is achieved by use of the SCinterface ePKI applet). Two form factors are available: a token with USB and NFC interface as well as a traditional smart card with contact and contactless interface. CardOS FIDO2 is a FIDO-certified application for CardOS smart cards, for using them as FIDO authenticator.
- **Evidian Web Access Manager:** The Evidian Web Access Manager supports a range of strong authentication methods, including certificate-based authentication and FIDO with token binding.

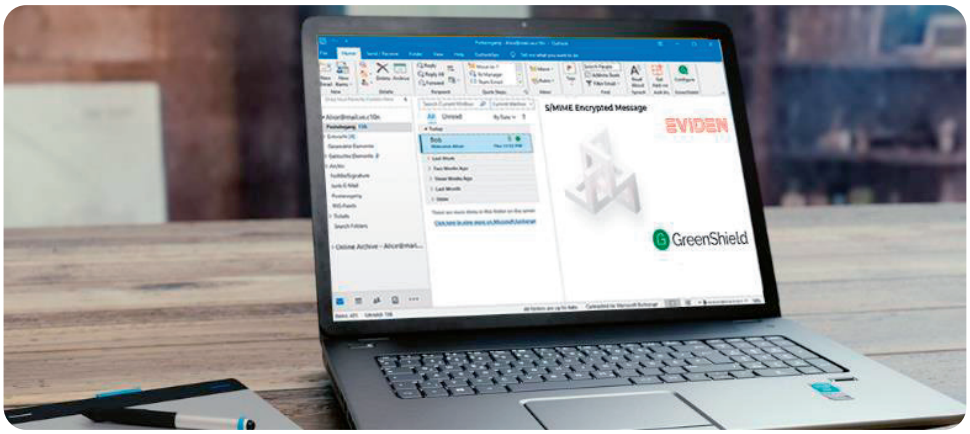


Figure 6: cryptovision GreenShield provides end-to-end email and file protection integrated in Outlook and Notes

Cryptographic email protection by Eviden

Eviden provides several powerful tools for email protection:

- **Cryptovision GreenShield:** cryptovision GreenShield provides end-to-end email and file encryption/signature seamlessly integrated in Microsoft Outlook and HCL (Lotus) Notes. Cryptovision GreenShield is approved for VS-NfD, NATO-, EU-restricted and EU classified information.
- **Cryptovision GreenShield Comfort:** This is a complete solution providing end-to-end encryption, PKI services as well as key and certificate lifecycle management controlled by automated workflows.

Phishing resilience is only one of several goals that can be achieved with these solutions

Eviden references

Eviden Digital Identity has two decades of experience with certificate-based authentication, PKI, and end-to-end Email encryption. The following list mentions a few customers

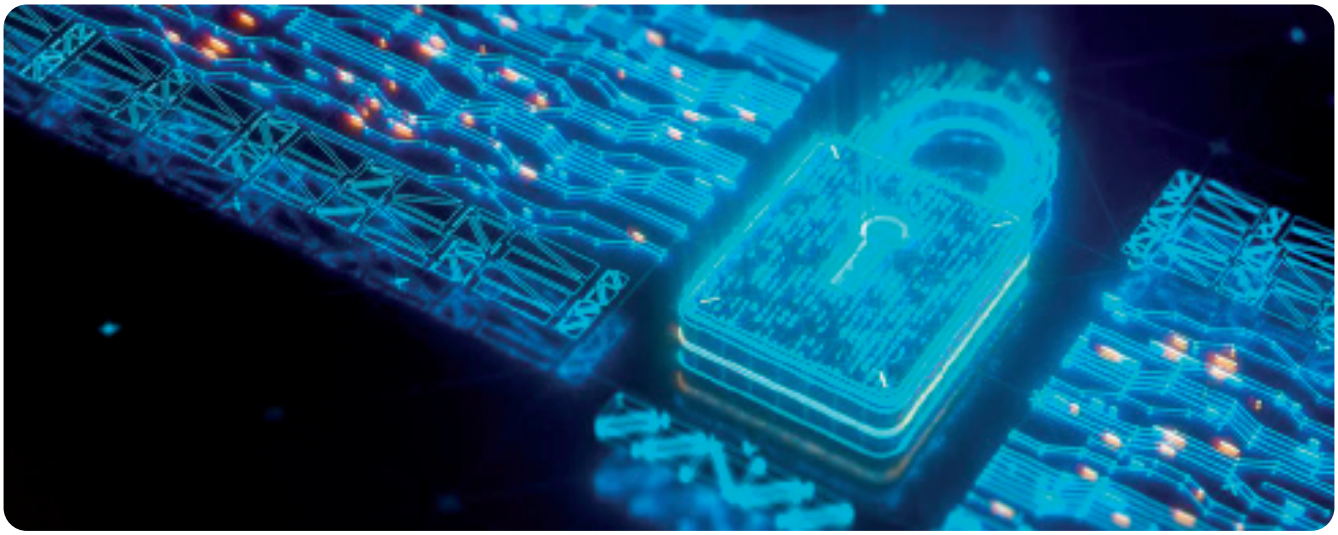
- **ADAC:** Certificate-based authentication
- **Airbus:** PKI solution
- **Allianz:** Certificate-based authentication, signature & PKI solution
- **BNP Paribas:** PKI solution
- **Bouygues Telecom:** PKI solution
- **Bundesministerium für Finanzen:** Secure email & PKI solution
- **Bundesministerium für Bildung und Forschung:** Secure email and PKI solution
- **Bundeswehr:** E-Mail security with cryptovision GreenShield Mail
- **City of New York:** PKI systems
- **Credit Agricole:** PKI solution
- **Deutsche Telekom:** Data & file encryption solution
- **e.on:** Certificate-based authentication and signature solution
- **EDF:** PKI solution
- **European Commission:** IDnomic PKI for intelligent transport systems
- **European Patent Office:** Certificates authentication and signature solution
- **Ministère de la Santé et de la Prévention:** PKI solution
- **Ministère de l'Éducation nationale:** PKI solution
- **Postbank:** PKI solution
- **SAP:** Secure email solution

Why investing in phishing-resilient technologies is critical

Phishing attacks often serve as the entry point for malicious actors to compromise an organization's network. Investing in phishing-resilient technologies therefore safeguards a company's digital assets & intellectual property.

Falling victim to a phishing attack not only exposes an organization to immediate financial and operational risks but also tarnishes its reputation. When customer data is compromised or services are disrupted, trust is eroded, and customers may seek alternatives.

The regulatory landscape surrounding data protection and cybersecurity is continually evolving. Numerous data protection laws and regulations, such as GDPR, HIPAA, and CCPA, impose strict requirements on organizations to protect sensitive information from unauthorized access or disclosure. Failure to comply with these regulations can result in severe financial penalties and legal consequences. Investing in phishing-resiliant technologies not only aids in compliance by preventing unauthorized access to sensitive data but also showcases an organization's dedication to meeting its legal obligations. This proactive stance can help avoid costly legal entanglements & regulatory fines.



Conclusion

In conclusion, phishing attacks represent a clear and present danger to organizations of all sizes and industries. By investing in cutting-edge phishing-resilient technologies, businesses can significantly reduce risks, safeguard their assets, maintain a pristine reputation, instill customer trust, and fulfill legal obligations. In the ongoing struggle against cyber threats, these technologies play a crucial role in strengthening the digital defenses of contemporary businesses, ensuring a secure, robust, and compliant future.

Eviden Digital Identity offers a compelling array of products and strategies that organizations can employ to enhance their resilience against the pervasive threat of phishing attacks. To find out more about our offering, please contact us here:

cv-info@eviden.com

www.cryptovision.com

Our consulting team will be happy to get in touch with you.

Eviden
cv cryptovision GmbH
Munscheidstr. 14
45886 Gelsenkirchen
Deutschland
Tel: +49 (0) 2 09 / 1 67 – 24 50
Fax: +49 (0) 2 09 / 1 67 – 24 61

EVIDEN

About Eviden[1]

Eviden is a next-gen technology leader in data-driven, trusted and sustainable digital transformation with a strong portfolio of patented technologies. With worldwide leading positions in advanced computing, security, AI, cloud and digital platforms, it provides deep expertise for all industries in more than 47 countries. Bringing together 53,000 world-class talents, Eviden expands the possibilities of data and technology across the digital continuum, now and for generations to come. Eviden is an Atos Group company with an annual revenue of c. € 5 billion.

[1] Eviden business is operated through the following brands: AppCentrica, ATHEA, Cloudamize, Cloudreach, Cryptovision, DataSentics, Edifixio, Energy4U, Engage ESM, Evidian, Forensik, IDEAL GRP, In Fidem, Ipsotek, Maven Wave, Profit4SF, SEC Consult, Visual BI, Worldgrid,

About Atos

Atos is a global leader in digital transformation with 105,000 employees and annual revenue of c. € 11 billion. European number one in cybersecurity, cloud and high-performance computing, the Group provides tailored end-to-end solutions for all industries in 69 countries. A pioneer in decarbonization services and products, Atos is committed to a secure and decarbonized digital for its clients. Atos is a SE (Societas Europaea) and listed on Euronext Paris.

The purpose of Atos is to help design the future of the information space. Its expertise and services support the development of knowledge, education and research in a multicultural approach and contribute to the development of scientific and technological excellence. Across the world, the Group enables its customers and employees, and members of societies at large to live, work and develop sustainably, in a safe and secure information space.

Connect with us

eviden.com

20231213