

H2 2024 Cyber Threat Report

# Decoding Deception: The Rise of AI-Driven Phishing Threats

January 2025

# Table of Contents

- 3 Introduction: Rising Challenges in Cybersecurity
- 4 Key Insights
- 5 Spotting Scams. Why It's Harder Than Ever
- 7 Inside the Minds of Cybercriminals: Common Fraud Tactics
- 10 2024 trends in online phishing
- 19 Targeted Attacks on Specific Sectors
- 26 The Network Edge: A Smarter Way to Stop Cyber Threats
- 27 Preparing for the Future: Rising to the Challenge of Cybersecurity

## Introduction

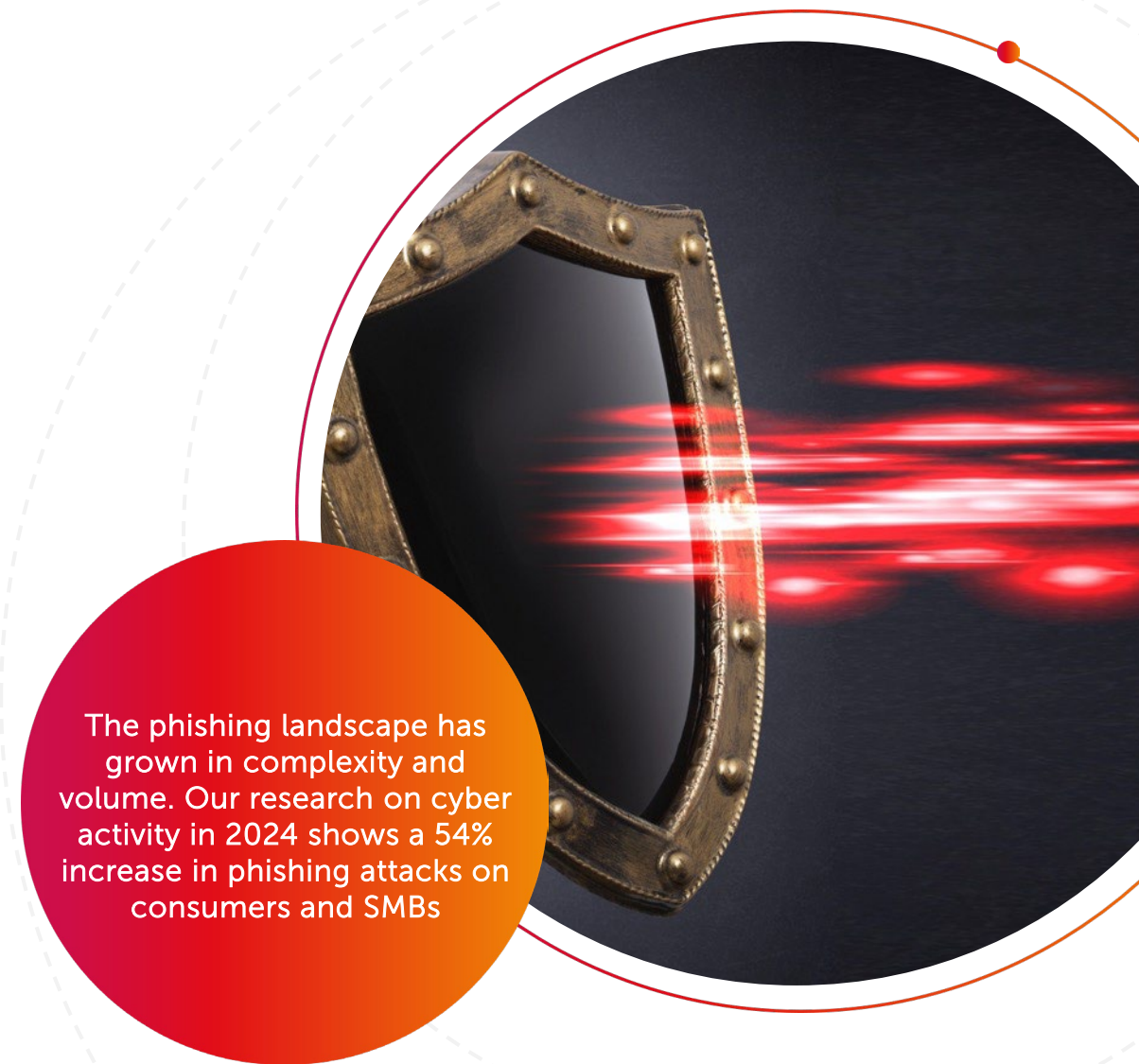
# Rising Challenges in Cybersecurity

The 2024 Allot Cyber Threat Report unveils that online fraud, particularly phishing, has become more sophisticated than ever, enhanced by the advancements in AI.

As attackers leverage AI to create realistic scams—like clone websites and personalized phishing emails—traditional trust indicators, such as HTTPS and SSL certificates, are no longer reliable. This report provides insights from Allot 2024 cyber protection activity in over 20 million consumers and SMBs worldwide and a deep analysis into the behavior of blocked domains on over 4 million selected subscribers protected globally, focusing on emerging threats like Phishing-as-a-Service (PhaaS), targeted attacks on high-value sectors, and psychological manipulation strategies.

Choosing the most representative examples from the use cases collected in our lab was a challenging task. Each example and cyber-related visual aid in this report belongs to real threats that have been blocked by Allot throughout the year, aiming to share authentic experiences of the everyday obstacles that regular users face in staying safe online.

In a world where even savvy users struggle to differentiate between legitimate and fraudulent sites, the need for robust, network-native cybersecurity solutions has never been more critical.



The phishing landscape has grown in complexity and volume. Our research on cyber activity in 2024 shows a 54% increase in phishing attacks on consumers and SMBs



# Key Takeaways

1

## Phishing Threats Evolve with AI

Attackers use AI to create realistic, tailored scams, including clone phishing and SEO poisoning, making detection harder.

2

## Phishing-as-a-Service (PhaaS) on the Rise

Subscription-based phishing kits and automated tools allow even unskilled cybercriminals to launch attacks at scale.

3

## Targeted Attacks on High-Value Sectors

These are especially attractive due to the valuable data and the volume of transactions. On the rise, we see Cryptocurrency platforms and Online Gambling, and as relevant as always, Parcel Delivery services.

4

## Social Engineering and Exploitation of Human Behavior

Cybercriminals manipulate online users to drive higher success rates by leveraging their trust in familiarity, urgency, and distraction.

5

## HTTPS and SSL Indicators No Longer Reliable

Scammers have perfected their techniques. Most hints and observation tips to identify a risky site are no longer valid.

6

## Secure network-native Protection Offers an Advantage

Real-time blocking of malicious domains ensures that users are protected from accessing deceptive sites, thereby reducing their risks.



2

## Spotting Scams: Why It's Harder Than Ever

# Spotting Scams

## Why It's Harder Than Ever

Online Fraud has advanced far beyond traditional methods, creating a sophisticated and challenging threat landscape. Before diving into the AI-driven features attackers seem to choose nowadays to design phishing campaigns, let's dive into the other three topics that are essential to today's scam ecosystem.

Many online fraud sites now use SSL certificates, showing the familiar "https://" and padlock icon, which users have been trained to associate with security. As a result, the traditional advice to rely on these indicators is no longer sufficient for identifying malicious sites.

The scope of online fraud has also expanded beyond email, which was once the primary attack vector. The Online Fraud activity analyzed for 2024 includes attempts across social media, in-app messages, regular search engines, and malicious ad redirections.

Another growing tactic is personalization. Scammers craft genuine, tailored messages using publicly available information, such as names or recent activities. Many times, malicious web trackers help to complete the online profile of victims, leveraging available information with their recent digital fingerprints. For instance, an email referencing a recent purchase or subscription can easily deceive users as it mimics real communications.

### Challenges of Modern Online Fraud Tactics



#### Blurring the Line Between Real and Fake

Online fraud sites often use "https://" (security padlocks icon) to appear secure, making the traditional advice to check for a secure connection less reliable as the sole indicator.



#### Scams Beyond Email

Once, most concerns were focused on email; however, online fraud attempts are now increasingly occurring through other platforms:

- Social media links
- In-app messages
- Advertisements with malicious redirects
- Collaboration tools (Slack, Teams)
- Gaming platforms



#### Tailored Attacks

Some online fraud campaigns use accessible information to personalize messages, making them harder to identify as scams. For instance, they may address the user by name or refer to a service recently used.



3

## Inside the Minds of Cybercriminals: Common Fraud Tactics

# Inside the Minds of Cybercriminals

## Common Fraud Tactics



### What is online fraud?

This term covers different deceptive activities carried out over the internet aiming to steal money, personal information, or other assets from individuals, businesses, or organizations. Fraudsters use various techniques to manipulate, deceive, or trick their victims into providing sensitive data or transferring funds. Let's explore the most common methods they use.



### Phishing

Phishing consist of deceitful emails, messages, or websites that mimic legitimate ones, aiming to trick users into sharing their sensitive data: passwords, credit card details, or personal information. In a broader sense, phishing often overlaps with Impersonation (Spoofing) and other online scams. In impersonation schemes, scammers pretend to be trusted entities—like banks or companies—using fake email addresses, websites, or even ads, blogs, and reviews to gain victims' trust. Among the most frequent scams detected through our protection services during 2024, we have Apparel Shopping Scams, Investment Fraud, Fake Job Offers, and Lottery/Prize Scams.



### Malware infections

Cybercriminals also use malicious websites, files, or apps to infect devices with malware. These infections allow them to gain unauthorized access to personal or business devices, stealing sensitive data and potentially causing further damage.



### Social Engineering

It's a key element present in each of the previous techniques. It plays a key role in manipulating human behavior to get them to reveal confidential information or perform specific actions.



# Other Forms of Online Fraud

Once cybercriminals obtain sensitive information, they often commit **Identity Theft** or **Credit Card Fraud**, further amplifying the damage.

Some scams take a more targeted approach, like **Spear Phishing** (targeted phishing aimed at specific individuals or companies) and **Vishing** (Voice Phishing using phone calls impersonating legitimate organizations to gain trust).

While these tactics are serious, they are not directly addressed by our network-native cybersecurity approach, which focuses on protecting mass-market users from threats like phishing and malicious websites.

## Why Focus on Phishing?

This report zeroes in on phishing because it's the most common type of online fraud impacting both individuals and small businesses daily. What is more, this type of threats are always lively in our user's mind. They find their self wondering if it's OK to open a message, use certain online fraud, or buying in website for the first time. By understanding phishing trends and tactics, we can better communicate the value of our Cyber protection solution and help them from falling victim to these increasingly sophisticated schemes.



4

## 2024 Trends In Online Phishing

# 2024 Trends in Online Phishing

Phishing attacks have recently evolved significantly, employing advanced technologies and sophisticated strategies to deceive users. Here are the key trends in online phishing for 2024:

## allot Secure

These evolving phishing tactics underscore the need for heightened vigilance and advanced security measures like Allot Secure to protect against increasingly sophisticated online threats. In the following pages, the report presents evidence of the current trends in phishing in the protection activity conducted by our service during 2024.

### AI-Enhanced Phishing

Attackers are utilizing artificial intelligence to craft highly convincing phishing emails and websites. AI enables the creation of personalized messages that closely mimic legitimate communications, making detection more challenging.

### Clone Phishing

Cybercriminals create nearly identical copies of legitimate websites or applications, a tactic known as "clone phishing." These clones are used to harvest sensitive information from unsuspecting users.

### Phishing-as-a-Service (PhaaS)

The emergence of new and easy-to-operate platforms has made phishing more accessible to cybercriminals. These services offer ready-made phishing kits, enabling even those with limited technical skills to launch sophisticated attacks.

### URL Spoofing and Lookalike Domains

Continues progress around perfecting the definition of URLs that resemble legitimate sites by misspelling names, using lookalike characters, or misleading subdomains.

### Phishing with SEO Poisoning

Scammers sharpened the use SEO tactics to rank fake websites in search results. Manipulating search algorithms to position fraudulent websites at the top of search results.

### Targeted Attacks on Specific Sectors

Certain industries, such as online gambling or crypto trade, have become prime targets for Phishing due to their high transaction volumes and valuable data. Attackers employ elaborate phishing schemes to exploit these sectors.

# Clone Phishing

## The Threat of Nearly Perfect Imitations

From all the different types of cyberthreats we studied in the recent months, Clone Phishing Websites are particularly dangerous. They are specifically designed to exploit online user's trust with the most deceiving look and feel.

Unlike traditional phishing websites, where we can find generic web designs or low-effort imitations, clone phishing websites are near-perfect replicas of legitimate sites. Some forgery sites are completely deceiving mimicking every single detail of the original one, from the layout and logo to even the smallest interactive elements.

The key is sophistication. Cybercriminals use a mix of technical expertise and advance AI tools to imitate and maintain convincing copies of official websites. Their goal is to create replicas so authentic that victims cannot distinguish them from the legitimate versions, increasing the likelihood of stolen credentials or other sensitive data.

Figure 1 shows the legitimate site for Outparks in Portugal, while the site below belongs to the exact clone site, "outparks-pt.site". As every detail was perfectly replicated, only those users with a cyber protection service preventing them from access will be able to avoid being fooled.



Figure 1



Figure 2

# Clone Phishing

## How AI Tools Keep Clones Up-to-Date With The Legit One



### Automated Website Cloning

Cybercriminals copy the design, layout, and content of the original page using website or script cloning tools. Results are sometimes outstanding, with replicas that are nearly identical to the original one.

The work is easier every day with tools, as AI-driven scraping is available for everyone. The new solutions use AI algorithms to extract and replicate every detail: logos, fonts, and interactive features like login forms. Furthermore, machine learning functions analyze the structure and code of the original site and make sure the clone result is as authentic as possible.



### Dynamic Updates

More AI tools and more difficulties to identify real from fake! As website content, especially from top brands for goods and services, the criminals need to apply more intelligence into the scam.

To do so, they use dynamic updates techniques that continuously pull live data from legitimate websites. With this, they make sure to reflect any changes in the legit website, such as new pages, campaign pictures or updated branding. Even if you are a frequent visitor to your favorite online store, it would be extremely difficult to notice the scam.



### Phishing Kits

To make things even scarily easier, a phisher rookie can go to the dark web and get a ready-made phishing kit template for his favorite websites.

The latest, more sophisticated versions are, of course, AI-powered, allowing cloning of the target website and capturing the victim's credentials.

Even more, some phishing kits also include AI-powered chatbots to interact with the users about customer support, making the user experience as deceiving as possible.



# Phishing as a Service (PhaaS)

## Crime Made Easy

Cybercriminals are increasingly turning to PhaaS (phishing as a service) platforms to access different phishing kits. They are subscription-based services that include the kits as part of a wider offer.

The growing threat of PhaaS is rapidly transforming the cybercrime landscape, posing a significant challenge for consumers and accounting for a substantial portion of Allot's anti-phishing activity in 2024.

Launching a Phishing attack was once limited to skilled hackers, but nowadays, it has become more accessible than ever.

PhaaS, ecosystem offering includes many different services:

- Phishing website hosting
- Phishing Kits libraries and customizations
- Email delivery
- Track interaction
- Customer support and step-by-step tutorials

This new reality, set a quite scary scenario where committing a very efficient crime is simple and easy to scale. More than ever, having a 24/7 updated protection solution is crucial.

A key indicator of PhaaS attacks is the Reused Template. Phishing kits utilize standardized designs, functionalities, and diverse elements across multiple phishing websites.

Figures 1 and 2 stopped last November, show a clear example of a reused template.

Figure 3

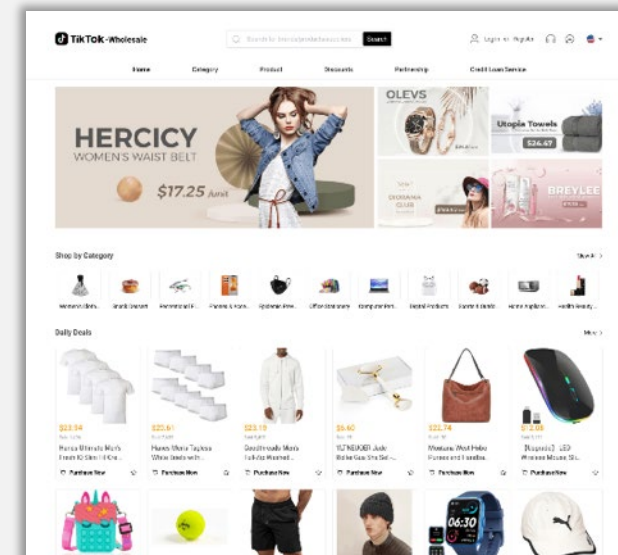
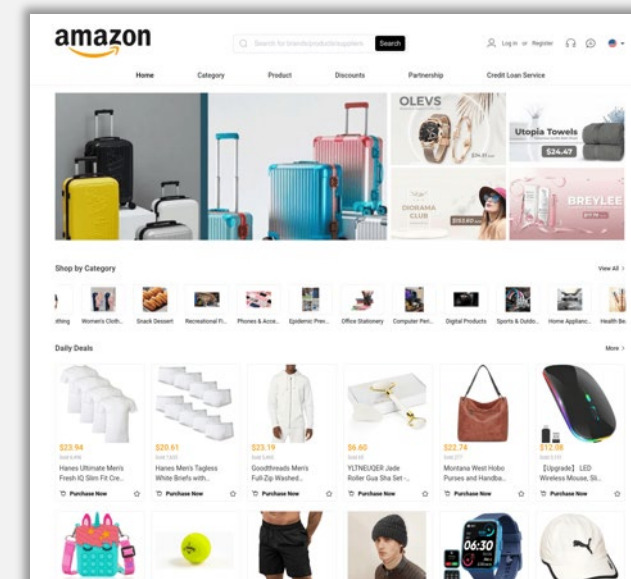


Figure 4





# Phishing in Style

Widespread Phishing attacks are a reality. For the last two years, we have seen increasing campaigns impersonating popular apparel, footwear, and clothing international brands.

Here is a short list of some we block for our protected customers:

- Puma
- Forever 21
- The North Face
- Lululemon
- Kickers
- Nike
- Guess
- Versace
- Asics
- Tory Burch
- COS
- Yves Saint Laurent
- Timberland
- Marc Jacobs
- Fjall Raven
- Salomon

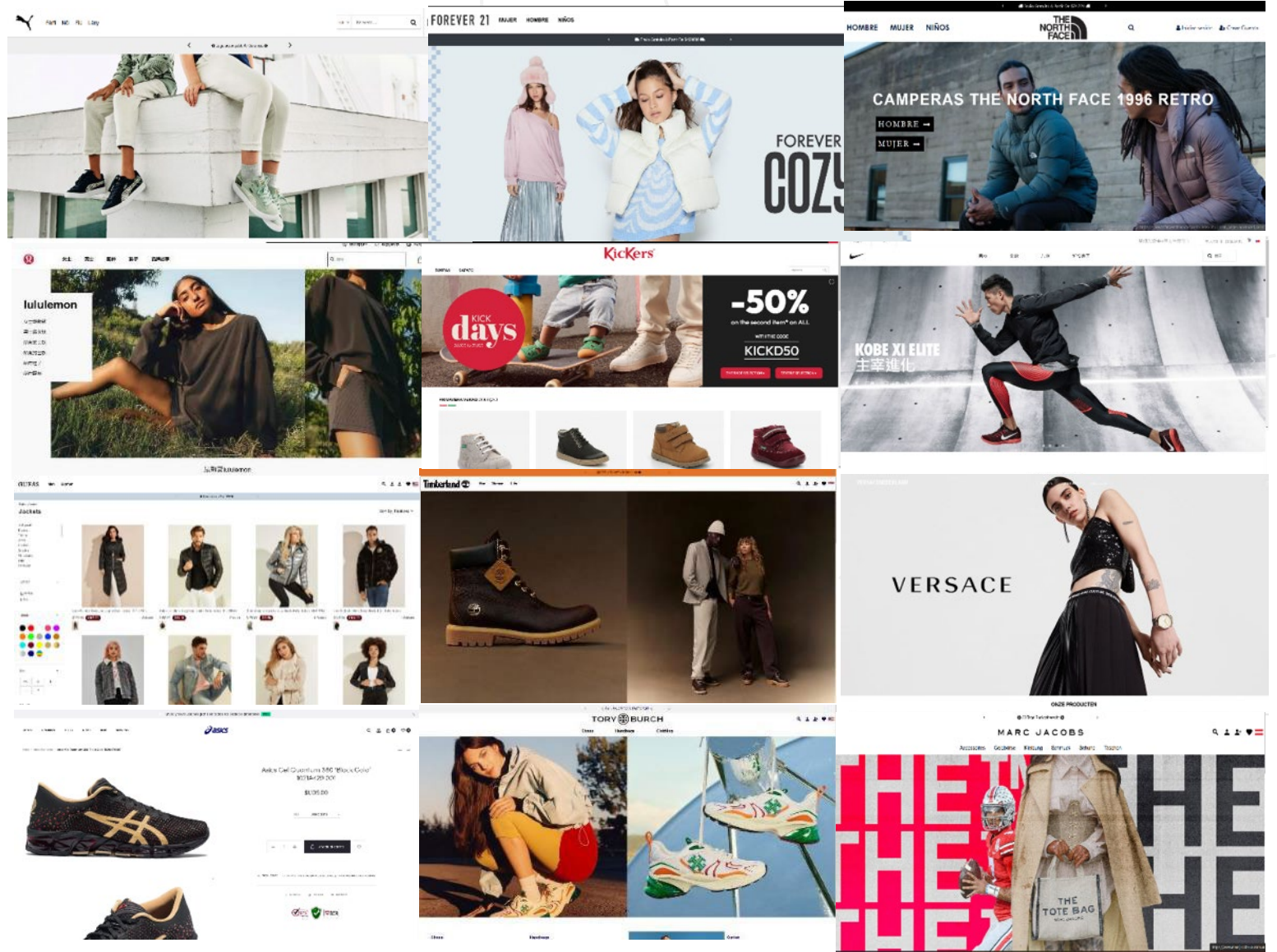


Figure 5

# Search and Deceive

## How Phishing Sites Rank High

We have already established that phishing sites can be highly deceiving, even for frequent visitors of legitimate websites. So, how to stay safe? The recommendations are clear: avoid too-good-to-be-true offers, carefully inspect URLs, and remain vigilant, especially when accessing the site from a blog or ad on social media, preferably using a trusted search engine as they continuously update their algorithms to detect and demote malicious sites.

But here are two main problems:

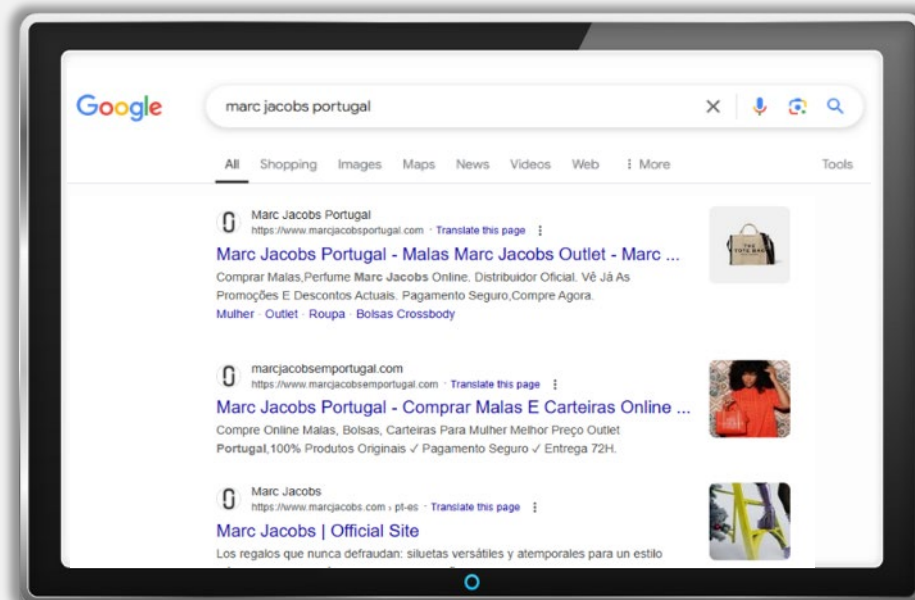
### Domain Spoofing

Attackers register fake domains that closely resemble the legitimate one, using tricks like substituting similar-looking characters (e.g., replacing "o" with "0") or adding subtle changes (e.g., "secure-login-bank.com" or "adidas-taiwan.com"). To make the site appear credible, criminals often secure SSL certificates, which display the padlock icon in the browser—a signal many users wrongly assume guarantees safety.

### SEO Tactics

It's not surprising for cybercriminals to leverage all well-known SEO tactics. In the case of phishing sites using advanced impersonating techniques, SEO will benefit from the expected elements (logo, titles, descriptions, etc.). Phishing campaigns may often include paid ads and sponsored links as a legitimate page. Other ways to increase rank potential are to buy expired domains with good reputations or use backlinks from other compromised or fake websites that may deceive the search engines.

Figure 6



### It's recommended to use a trusted search engine

However, despite their continuously updated algorithms, verified phishing sites rank right after the legitimate ones, even if they are not newly registered.

In the example in Figure 6, the legit sites rank three only after two phishing sites.

### To remain safe, users should carefully inspect the URLs

But is it so easy? Here's some of examples from recent protection activity:

- amazonshop.cc
- shein.at
- tupperware-us.com
- kurierfedex.pl

# The Psychology of Phishing


## How Scams Exploit Human Behavior

Phishing involves more than just advance technical achievements; it will always be a psychological one. Phishing attacks are a prime example of social engineering, a tactic that manipulates human behavior to achieve malicious goals. By exploiting trust, distraction, and urgency, phishing schemes target emotional and cognitive vulnerabilities, making it easier to deceive users and compromise their information..



### Trust in Familiarity

One key element of phishing is leveraging trust in familiarity. Humans tend to trust emails or websites that appear legitimate, especially when they mimic well-known brands or services. Scammers use social engineering techniques to create fraudulent emails and websites that look identical to official communications from trusted organizations, such as online retailers or banks. These messages often request order confirmations or login credentials, exploiting the user's familiarity with the brand to lower their defenses.



### Distraction and Multitasking

Another cornerstone of social engineering in phishing is distraction and multitasking. In today's fast-paced digital environment, most online interactions occur on mobile devices, often while users are on the go. Whether checking emails during a commute or shopping between tasks, users are frequently distracted, which reduces their ability to notice subtle red flags in a phishing message. Scammers rely on this lack of focus, knowing that a distracted individual is more likely to fall for their trap.



### Urgency and Pressure

Phishers also masterfully employ urgency and pressure, key tools in social engineering. Messages warning of account suspensions, fraudulent activity, or time-sensitive offers are designed to create panic, forcing users to act without carefully analyzing the situation. By inducing fear or urgency, scammers push victims to bypass their usual caution and comply with malicious requests.



# Hiding Malicious Links

To complete cybercriminals' most updated toolkit ideas, we should include the most common practice to hide malicious URLs: using URL shorteners to mask malicious links and evade detection.

These tactics are often combined with:

- **Social media** and messaging apps where shortened URLs appear less suspicious.
- **Time-delayed redirects**, where the link initially points to a harmless site but, after a few seconds, redirects to a malicious page.
- **QR codes**, where the shortened link is embedded, making it impossible for users to verify the destination URL before scanning.

This strategy exploits user trust and makes it harder to identify phishing attempts.



5

## Targeted Attacks on Specific Sectors



# Bet and Beware Fake Sites in the Gambling Industry

Online Gambling is another online industry with all the elements for a good business model for cybercriminal phishing scams. In particular, the online sports betting market is experiencing significant growth worldwide. The new online platforms make it easy for more users to participate from home or on their phones. Another reason to attract users is the variety of sports events and betting options, such as live streaming and in-play betting. The latest figures show that the number of users worldwide duplicated in the last 5 years, reaching almost 140 million by the end of 2024.

Online betting platforms generally request and verify a large amount of personal data, including full name, date of birth, address, and sometimes even the social security number. Additionally, when placing a bet, the user must make a deposit, so users need to share sensitive financial details from debit cards and eWallet systems. The data stolen from online victims is frequently used to commit further frauds such as identity theft and unauthorized online purchases.

Scammers leverage the urgency and real-time nature of the sports events to lure users into the fake platforms. Just before or during a major sports event, they launch phishing email campaigns and social media ads offering "exclusive bonuses" on their next bet. When clicking on those links, they reach the fake website, where everything is ready to capture the victim's data.

## Recent examples of Phishing site impersonating Top Online Betting Platforms worldwide:

- 9 mimics 22bet (Top EU)
- 10 mimics Sbotop (Top APAC)
- 11 mimics BetMGM (Top NA)

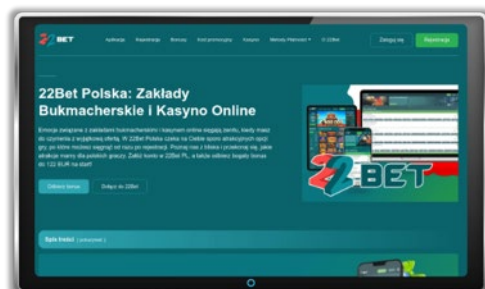


Figure 9

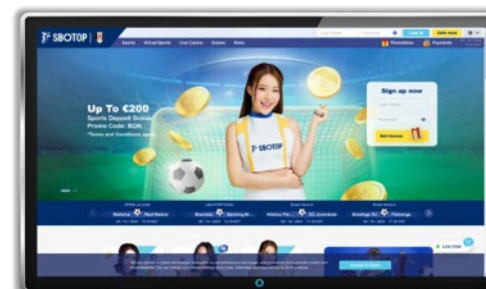


Figure 10

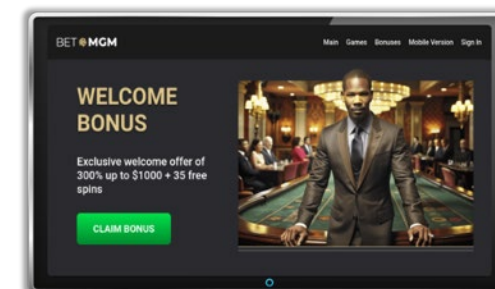


Figure 11



# Fake Deliveries, Real Risks

## Phishing in Everyday Life

Phishing attacks are not limited to those sectors with billion-dollar-a-day transactions; scammers can also profit from targeting other everyday online activities such as shopping or parcel deliveries.

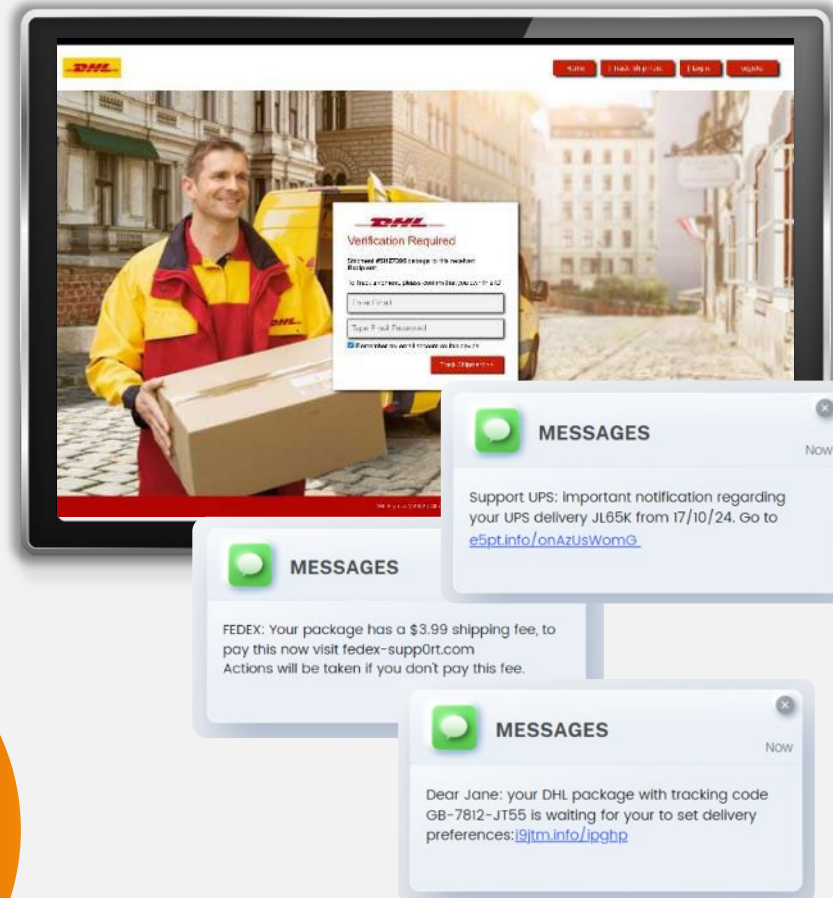
A trend that never gets old is phishing attacks behind fake shipment tracking notifications to dupe online users.

These scams are particularly effective as they rely primarily on a sense of urgency and familiarity. Most people in today's world are likely waiting for parcel delivery within the next day and are used to getting legitimate text messages that are very similar to fake ones.

Using all the mimic techniques we analyzed earlier, the links included in the text messages will show users a page with the expected look and feel. The actions requested will usually involve sharing personal information and address or payment details in relation to shipping fees.

Familiarity in a habitual transaction makes staying alert to unexpected messages difficult. Once again, remaining safe and avoiding falling for this type of scheme is challenging for regular users. A network-based protection solution is critical in identifying malicious domains in real time and in stopping users from accessing phishing sites.

Social engineering 101  
Exploiting basic human behavior such as Trust in Familiarity and Urgency, cyber criminals prompt online users to access the links and sites without analyzing their authenticity.



# Crypto Fraud

## The Art of Deception

When investigating **Targeted Attacks on Specific Sectors**, there's one that escalates to the top: **Cryptocurrency fraud**. The scams are notorious worldwide; just in the USA, the Federal Trade Commission (FTC) announced that crypto fraud has one of the highest losses per consumer and accumulated \$679 during the first half of the year.

2024 saw numerous high-profile scams. This section uncovers common tactics scammers use and how they exploit advanced phishing techniques

How does the typical crypto scam work? Here are the key elements to consider:

### Multiple channels attracting victims

A characteristic aspect of several crypto scams is that they lure uninformed victims with **Deepfake or Voice-dubbed Videos** exploiting the popularity and credibility of well-known celebrities. Using Gen-AI, scammers create convincing videos featuring personalities like Elon Musk, Bill Gates, or Warren Buffet talking in public interviews, recommending the investment, guaranteeing high returns, and endorsing fictitious Bitcoin giveaways.

The deceptive videos were spread all over **social media** platforms (Facebook, Ticktock, Instagram), luring the victims to malicious sites. They use targeted

advertisements to tailor specific demographics with higher engagement rates. They **use hashtag campaigns** related to the celeb or crypto trying to make the videos go viral among specific communities.

Additionally, they pushed email campaigns, personalizing the messages with known user information.

Once more, social engineering played an important role, using psychological tricks to hence emotions. In particular, **urgency** and or **fear of missing out (FOMO)** are linked to the unique moment to take the opportunity to act and become investors.



# Fake Platforms. Perfect Illusions.

Fraudsters create convincing near-identical replicas of legitimate crypto trading sites, using AI-driven tools to match the real ones regarding content, design, and features, including many references to security measures, regulatory certifications, etc.

The interfaces look polished, showing perfect dashboards to track, trade, and buy different cryptocurrencies to mimic authenticity.

On many occasions, there is evident **re-use of phishing templates**, as we previously discussed for Phishing-as-a-Service. This is the case of platforms such as wedexy.com, dewoxed.com, fuext.top, and many others. Among the malicious blocked sites throughout the year, we found the same scams replicated hundreds of times. The cybercriminals do this to avoid detection and continue their massive reach fraud campaigns. They maintain libraries of video templates and designs. When necessary, they just changed the domain name and include it in the corporate branding, giveaway promotions, and fake celebrity pitches while keeping the core psychological hooks and technical sequence unchanged.

*Successful scammers always know when to retire from the scene, in this case, they just renew the brand and domain name and start over.*



Figure 7

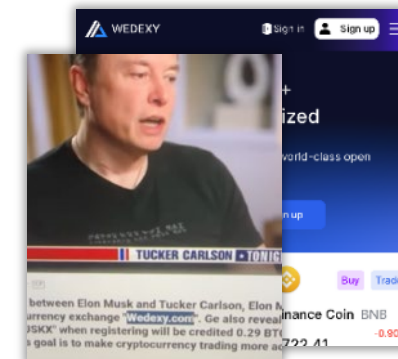
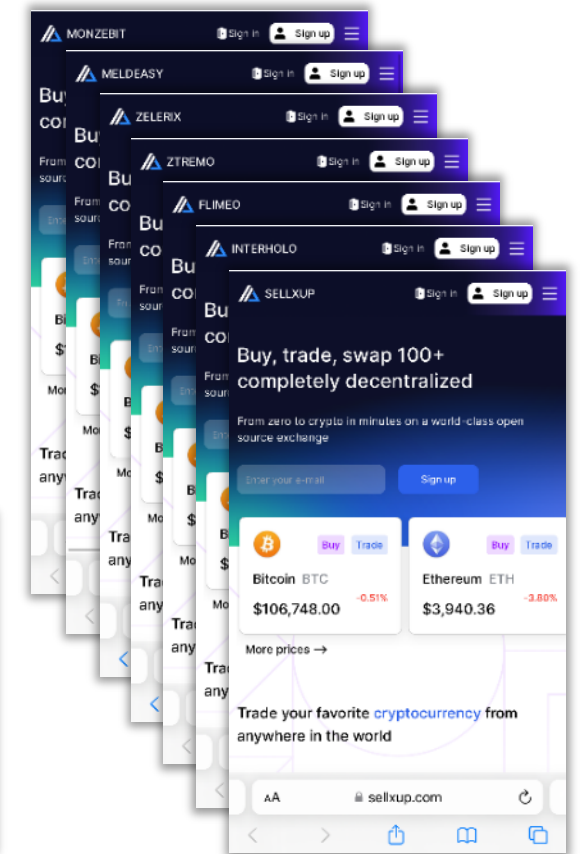


Figure 8



# Scam Execution.

## From Trust to Theft.

Unlike usual phishing attacks aimed to steal sensitive data as soon as the victim shares it, in most of the Crypto Scams analyzed involve prolonged interactions to gain trust, encourage more significant investments and generate higher profits.

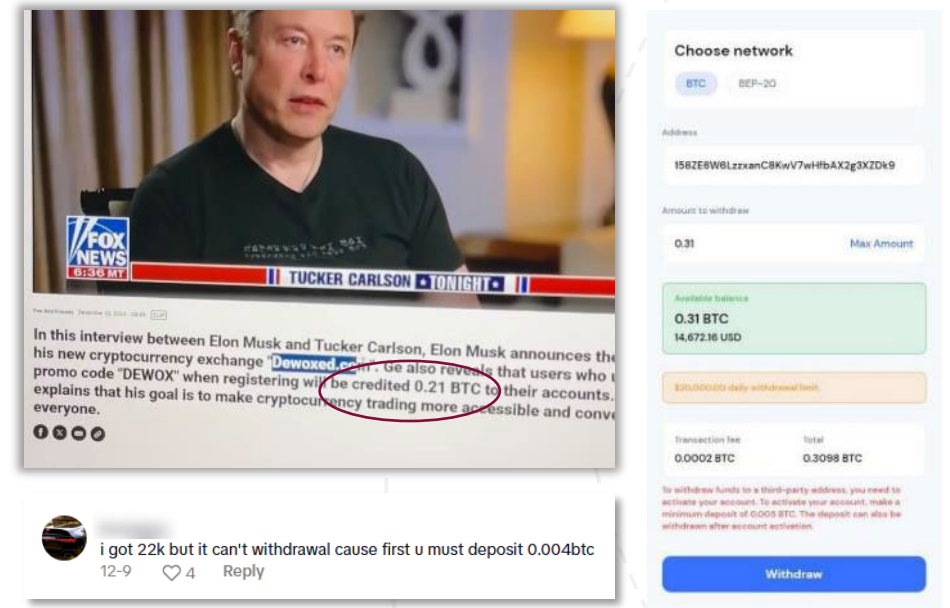
Once the victims are in the fake crypto platform, they are encouraged to deposit cryptocurrency with promises of high returns. Very fast, the initial profits are shown on the dashboard to entice further deposits, but once the accounts have significant funds, the withdrawals stop working.

Returning to the 2024 example of celebrity's deepfake videos, the use case mostly concerns **crypto giveaways**. The deep-faked celebrities describe a unique Bitcoin giveaway opportunity in collaboration with the fake platform; they provide a **promotional code** and step-by-step instructions on how to claim the free Bitcoin funds in the new account.

### Magic is in progress!

Immediately after signing in and entering the promo code, the users have a positive **Bitcoin balance**, let's say 0.21 BTC (about \$30,000 by December 2024): hocus-pocus!

However, there's a small trick when they try to withdraw the money. As expected, users need to share the crypto wallet (or credit card, Paypal details) when ordering the withdrawal; the platform will **charge a minimum** amount to activate withdrawal capabilities (0.005 BTC = about \$500). Scammers immediately steal the charge and never provide the withdrawal to the victims. Eventually, after they make enough money, the communication campaign and platform **disappear**, leaving the victims without the possibility of recovering their money.





# Conclusions

## AI-Driven Scams and Future Challenges

Most of the time, scam stories have a repetitive formula: a promise of extraordinary gains, a unique opportunity with a time limit to get it, and the need to invest a little to gain a lot.

So, what is new in this scenario?

If online scams are more effective today than ever, is due to the exploitation of all the advantages that AI-enhanced phishing brings to the game:

- Perfect design of emails and websites.
- AI-generated content mimics legitimate websites, such as fake user testimonials and dynamic updates.
- Phishing as a Service (PhaaS) with easy-to-use kits allowing scammers access to modern tools to escalate the attacks with lower effort.

We also need to consider AI-generated assets that contribute to reach credibility and access to specific targets:

- Realistic AI-generated videos featuring personalities that promote the scam..
- Ads tailored to specific demographics, ensuring higher engagement rates.
- Automation through bots that manage ad placement and user interactions at scale.

People falling for new and attractive scams will continue to happen as psychological manipulation always works its magic.

However, as most of these scams happen online, cybersecurity services have an important role in ensuring that the continuously updated solution prevents naïve users from accessing the malicious scam sites.



# The Network Edge.

## A Smarter Way to Stop Cyber Threats.

All phishing trends point to a sharp continuation of deception and effectiveness in their practices. More than ever, online users need help to stay protected.

Network-native cyber protection solutions play a critical role in protecting over 20 million consumers and SMBs worldwide. The security service operates seamlessly in the background, detecting and blocking malicious links in real-time before users can access them, unlike traditional endpoint security measures that rely on user action or software updates.

This proactive approach neutralizes even the most sophisticated threats, such as AI-generated clone websites and malicious domains disguised behind shortened URLs. By blocking these dangers at the network level, the solution eliminates the need for individual vigilance, which can often fail when users are faced with urgent, personalized, or highly convincing scams.

The system is updated continuously, 24/7, without any intervention required from the user, which is key to quickly adapting to emerging trends and newly launched campaigns. Using advanced algorithms and threat intelligence, it constantly analyzes all internet connections of protected devices, keeping customers protected from online fraud, including those targeting high-risk industries like cryptocurrency, gambling, and parcel delivery services.

Network-native protection is also ideal for environments with multiple devices. Users can access the internet using smartphones, tablets, or home networks without installing or configuring software on each device individually.

This way, threats are stopped at the network level, protecting sensitive information, reducing malware infections, and enhancing overall security for individuals, families, and businesses.





# Preparing for the Future.

## Rising to the Challenge of Cybersecurity.

For many years, Allot Cyberthreat Reports has shown a tremendous evolution in the methods and advanced technology cybercriminals use to target their victims. As we focus our studies on the online protection of consumers and SMBs, several times in the past, we highlighted how regular online users constitute a desirable segment to target and how the advanced methodology used to attack large enterprises translates to minor victims on a mass scale.

What is new for this year's report? The 2024 report highlights how cybercriminal are increasing their efforts to deceive online users. In this sense, the goal is not to sneak an antivirus installed in the device or take advantage of an outdated operative system. Artificial intelligence-driven sophisticated tactics make phishing attacks much harder to detect, increasing the vulnerability of potential victims.

As we move into 2025 and beyond, cyber threats will increase the challenge, and the need for real-time protection has never been more urgent. The battle against cybercrime is ongoing, but with robust measures in place, Telecommunication Service Providers are well-equipped to protect individuals, families, and businesses from harm.



# References

- Obaloluwa Ogundairo, Peter Brooklyn. (2024) AI-Driven phishing detection systems. ResearchGate. Retrieved from [https://www.researchgate.net/publication/382917933\\_AI-Driven\\_Phishing\\_Detection\\_Systems](https://www.researchgate.net/publication/382917933_AI-Driven_Phishing_Detection_Systems)
- Schaffer, N. (2024). AI website scraper: Benefits, dangers, and best practices. Neil Schaffer. Retrieved from <https://nealschaffer.com/ai-website-scraper/>
- Trustwave SpiderLabs. (2024). Why do criminals love phishing-as-a-service platforms? Trustwave Blog. Retrieved from <https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/why-do-criminals-love-phishing-as-a-service-platforms/>
- Cimpanu, C. (2023). Massive phishing campaign uses 6,000 sites to impersonate 100 brands. BleepingComputer. Retrieved from <https://www.bleepingcomputer.com/news/security/massive-phishing-campaign-uses-6-000-sites-to-impersonate-100-brands/>
- HackRead. (2024). SEO poisoning: How scammers trap users via search engines. HackRead. Retrieved from <https://hackread.com/seo-poisoning-how-scammers-search-engines-traps/>
- Neko Papez (2024) URL shortening allows threats to evade URL filtering and categorization tools. Menlo Security. Retrieved from <https://www.menlosecurity.com/blog/url-shortening-allows-threats-to-evade-url-filtering-and-categorization-tools>
- Grauer, Y. (2016). Five reasons you should stop shortening URLs. Forbes. Retrieved from <https://www.forbes.com/sites/ygrauer/2016/04/20/five-reasons-you-should-stop-shortening-urls/>
- Statista. (2024). Worldwide online sports betting user statistics. Statista. Retrieved from <https://www.statista.com/outlook/amo/online-gambling/online-sports-betting/worldwideusers>
- The Motley Fool. (2024). Crypto investment scams: Trends and red flags. The Motley Fool. Retrieved from <https://www.fool.com/research/crypto-investment-scams/>
- New York Times. (2024, August 14). Elon Musk AI deepfake scam: How cybercriminals use technology to deceive. The New York Times. Retrieved from <https://www.nytimes.com/interactive/2024/08/14/technology/elon-musk-ai-deepfake-scam.html>



# About Allot

Allot Ltd. (NASDAQ: ALLT, TASE: ALLT) is a provider of leading innovative network intelligence and converged security solutions for service providers and enterprises worldwide, enhancing value to their customers. Our solutions are deployed globally for network and application analytics, traffic control and shaping, network-native security services, and more. Allot's multi-service platforms are deployed by over 500 mobile, fixed and cloud service providers and over 1000 enterprises. Our industry-leading network-native security-as-a-service solution is already used by many millions of subscribers globally.

For more information about how Allot Secure can protect communication service provider's consumer and SMB customers, visit [Allot Security Solutions](#)



© 2025 Allot Ltd. All rights reserved. Specifications subject to change without notice. Allot and the Allot logo are registered trademarks of Allot. All other brand or product names are trademarks of their respective holders.