allot
See. Control. Secure.

Don't Get Phished!

SMB & Consumer Handbook

Intro

Phishing remains one of the most common and effective tools used by cybercriminals to gain access to personal information. Gmail alone blocks more than 100 million phishing emails per day, and 68% of them are new variations. This is not surprising as they are simple, low-tech, and exploit weaknesses in human nature to target everyone – individuals and organizations. Phishing continuously evolves to evade detection and, using advanced social engineering techniques, is getting more sophisticated than ever.

Even though the threat is so widespread and growing, 45% of internet users don't understand what phishing is or the risks associated with it. As phishers use different psychological tricks and human emotions (like urgency or fear of missing out) to trick people into clicking, it's important to educate yourself on phishing methods and stay updated on the latest security best practices.

The practical tips in this handbook will help protect your customers and you against phishing and teach you how to spot even the most well-crafted of phishing emails.

allot

How Phishing Works

Phishing describes messages that appear to come from a trusted entity, but are actually from cybercriminals attempting to trick victims into giving away their personal data, such as login credentials and financial account numbers. These messages contain links to fraudulent websites designed to look real – most commonly, they impersonate banks, retailers, and popular internet services, such as Amazon, Facebook, or PayPal.

In phishing, there are two common attack scenarios with two distinct goals:

Steal credentials

1. User gets a phishing message.
2. User clicks on a link.
3. User provides his credentials on a legitimate-looking phishing site.
4. Hacker gets credentials.

- Hacker steals money from user's bank account/ credit cards.
- Hacker sells the data on the darknet.
- Hacker uses credentials / identities to commit other cybercrimes.

Plant malware

User gets a phishing message.

User opens a malicious attachment.

Device is infected with malware/ransomware, cryptojacking, banking Trojans, etc.

- Hacker steals money / data via malware.
- Malware encrypts user's files and demands a ransom (ransomware).
- Phishing was an initial vector of the attack – hacker gets access to the corporate network to start an attack on the organization – to steal data or money.

How to Spot Phishing Email

Phishing messages typically contain some common elements described below, so look out for these elements as “red flags” when checking your email.

Official-looking graphic

Phishing emails can contain official looking logos or signatures of the impersonated organizations or their employees - scammers can easily access them from websites. Don’t think the email is legitimate simply because it includes an official-looking graphic.

“Dear Customer” instead of your name

The scammers typically send these emails out by the thousands in hope that some will reach real account holders of specific companies.

Request for personal information

Any message that asks for your personal information is suspicious and can be a phishing attempt.

One of the popular subject lines

The most common subject lines used in phishing emails targeting businesses are ‘Request’ (accounting for over a third of all the phishing messages), followed in popularity with ‘Follow up’, ‘Urgent Important’ or ‘Are you available? / Are you at your desk?’*. They show how hackers are exploiting urgency, personalization and pressure to trick victims into clicking on malicious links.
Many of the email messages also refer to finance and payments with popular subject lines being ‘Your bill is ready’, ‘Payment status’, ‘Purchase’, ‘Invoice’, ‘Direct Deposit’, ‘Payroll’ and others.

Sense of urgency and account status threat

In many cases phishing emails warn of a sudden change to an account, refer to an urgent change in a delivery, or may present an unusually high bill – which is designed to send users into a panic and to click on malicious links.

Forged email address

The sender’s email address may be forged, even if it looks legitimate, e.g. represents email from the bank.

Unprofessional email title, bad grammar and typos

Some phishing emails are easy to spot as they can sound unprofessional and contain exclamation marks, use poorly written sentences, bad grammar, misspelled words - nothing that legitimate organizations would typically use in their official communications to customers.

Disguised or modified link

Even though a web address may seem to contain an official address of the organization it may not be a legitimate website. When you hover your mouse over a link, the actual URL you are being directed to is displayed in a popup or at the bottom of your browser window. If the link in the email and the URL displayed are not identical or it looks suspicious, there is a possibility that you are being directed to a fraudulent site.

* 2019 Spear Phishing Report, Barracuda

How to Protect

With phishing attacks on the rise, it's important to stay on top of the best practices on how to protect yourself and minimize risks. Here're some helpful tips.

Get cybersecurity protection

Subscribe to a cybersecurity service from your telecom operator that provides robust mobile cybersecurity protection against various online threats, including phishing. Allot Secure is the world's leading operator-delivered, network-based, cybersecurity solution for fixed and mobile networks.

Carefully check the sender's address, URLs and other elements in the email

Develop a habit of hovering over URLs to check where they lead and check the spelling of email addresses. When in doubt, research and contact the sender independently to verify an email is legitimate. Taking a few minutes to make a quick call or open a chat message to the sender can reduce your risk and help protect your data. The ability to spot minor differences in emails can make a big difference for your security. Great learning exercises for this are online phishing quizzes where you can test yourself – like, for example, this one created by Google.

Use the browser address bar

Instead of clicking a link in an email, go directly to the company's website and sign in there to see if there are any signs of unusual activity in your account. If you're concerned, change the password.

Check writing style

Remember that legitimate organizations use professional language and typically don't make spelling or grammar mistakes.

Update regularly

Don't forget to regularly install updates for your operating system, antivirus, browsers, Adobe Flash Player, Java, and other software. Cybercriminals frequently use known exploits, or flaws, in your software to gain access to systems.

Use two-factor authentication

Wherever possible, enable two-factor authentication. This will make it harder for hackers to access your online accounts even if they manage to steal your credentials.

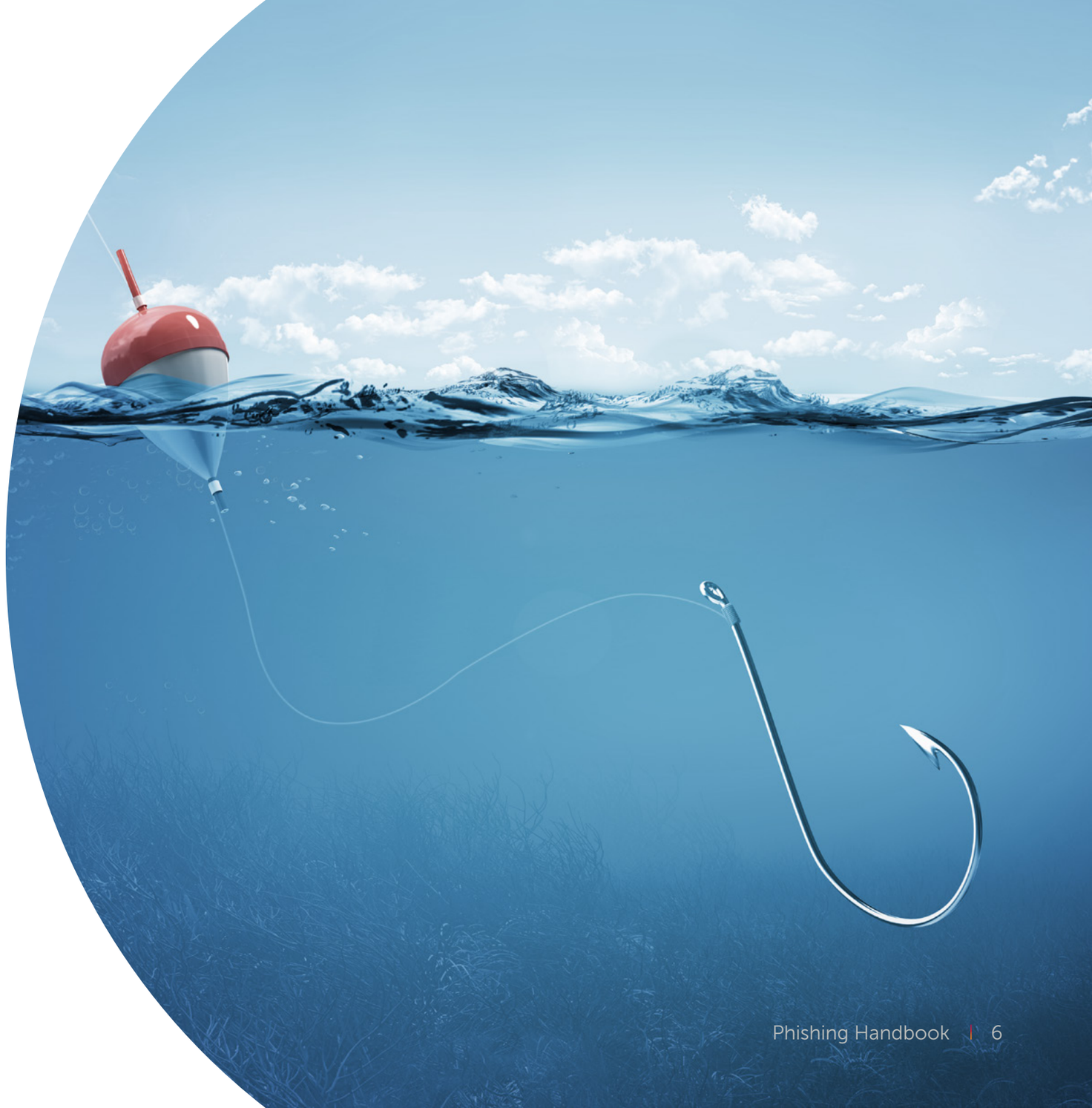
Avoid oversharing online

Take special care when sharing information online on Facebook, Twitter, LinkedIn and Instagram. Details such as birthdays, hobbies, holidays, job titles, promotions, and relationships can all be used by cybercriminals to craft more sophisticated phishing attacks. Don't use security questions or passwords that can be found easily on social media, like your dog's name or your mother's maiden name.

Conclusion

Phishing attacks are successful because they exploit the weakest link in the security chain – the human factor. By applying the security tips described above, you can learn to recognize phishing emails and minimize the risks of getting caught “on the hook” by cybercriminals.

Always stay alert online, rely on common sense, and maintain a healthy level of suspicion to everything you get in your mailbox or private messages on social media. Remember the simple fact - organizations don’t send emails asking customers to provide their credentials and other personal information. Know the “red flags”, think before you click, double check the sender address, and be extremely cautious when entering your passwords or sensitive financial info.



allot

About Allot

Allot Ltd. (NASDAQ, TASE: ALLT) is a provider of leading innovative network intelligence and 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-based 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-based security as a service solution is already used by over 20 million subscribers around the world. Allot. See. Control. Secure.
For more information, visit AllotSecure solutions.

Sep 2023