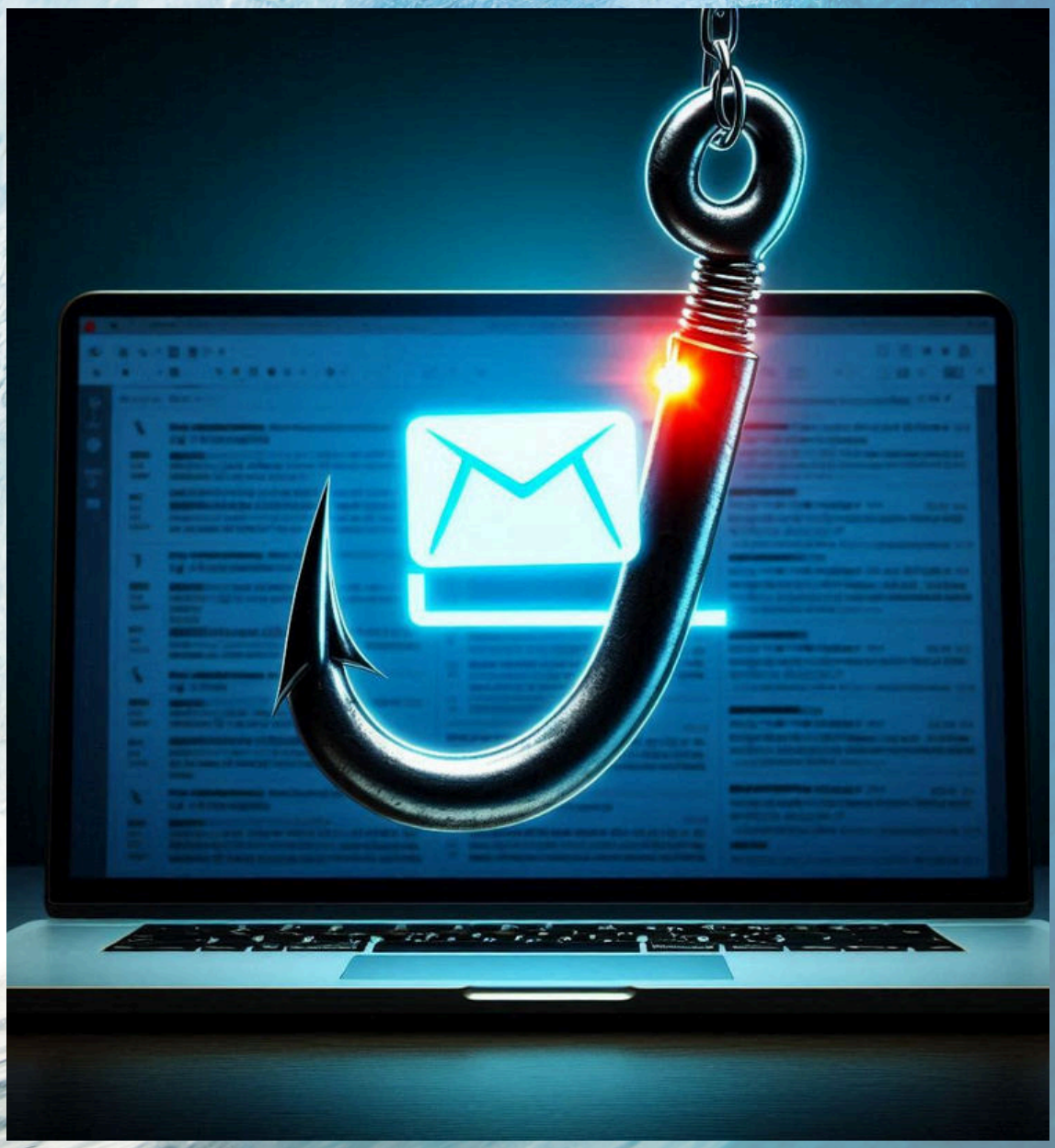
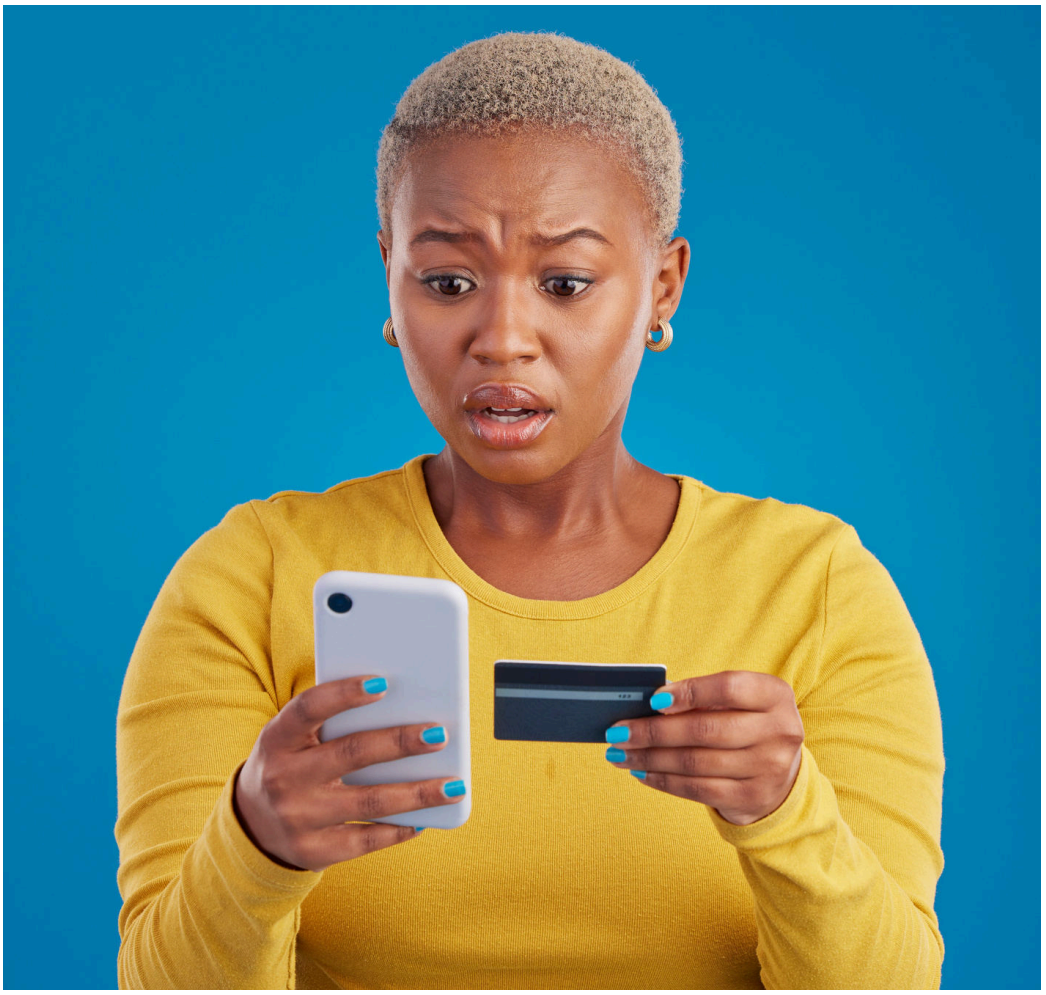
# HOW TO NAVIGATE THE WATERS OF PHISHING ATTACKS



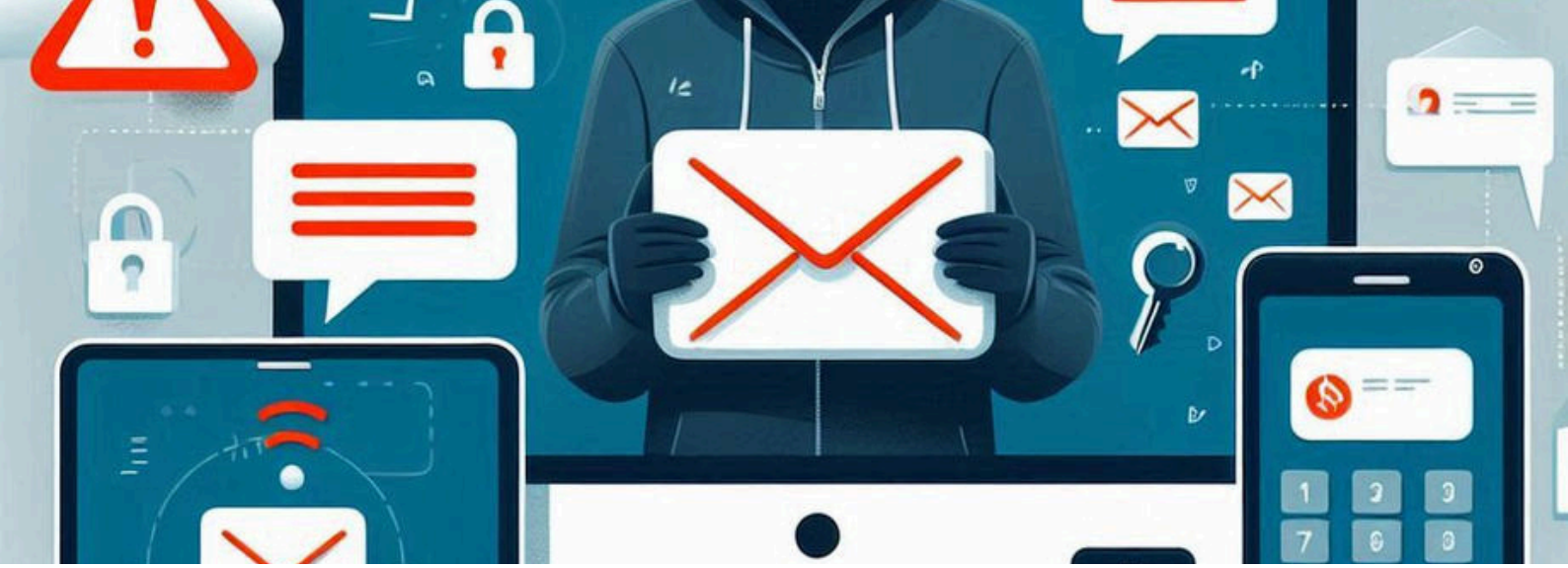
www.safewiz.eu

# WHAT IS PHISHING?



Phishing, a cyberattack method, derives its name from the word "fishing," symbolizing how attackers "fish" for sensitive information by casting an attractive lure

These scammers often pose as familiar faces, like your bank or a popular e-commerce website, to trick you into sharing personal details - things like your password, credit card info, or login credentials. They might claim there's an urgent issue, like a security problem or a locked account, or even an incredible deal, making it seem like you have to act fast.



# COMMON PHISHING TECHNIQUES

---

**SMISHING - SMS PHISHING**

Phishing through text messages, where attackers send links to malicious websites or prompt calls to fraudulent numbers, aiming to steal information or install malware.

**EMAIL PHISHING**

Attackers send deceptive emails that appear to be from legitimate entities, like banks or colleagues, to trick recipients into revealing personal information or clicking malicious links.

**CLONED WEBSITES**

Attackers create exact replicas of legitimate emails or websites, slightly modified to include malicious links or attachments, deceiving victims into believing they are authentic.  They capture your login credentials or payment information once you enter it.

# COMMON PHISHING TECHNIQUES

---

**SPEAR PHISHING**

Highly targeted attacks where attackers gather information about the victim to create personalized and convincing messages, increasing the likelihood of success.

**SOCIAL MEDIA ENGINEERING**

Social Media Engineering is a form of phishing where attackers manipulate or impersonate people on social platforms to extract personal or sensitive information. Attackers may pose as SM Support, friends, colleagues, or influencers to gain trust before asking for data or money.

**VISHING - VOICE PHISHING**

A deceptive tactic where scammers use phone calls to trick victims into providing sensitive information or money. Elderly are usually targeted by vishing.

# THE COSTS

01

### Financial loss

Phishing attacks can lead to significant financial damage through fraudulent transactions or data theft.

02

### Reputation Damage

Companies hit by phishing attacks often suffer reputational damage, losing customer trust and loyalty.

03

### Data Breaches

Compromised personal or corporate information in phishing attacks can lead to widespread data breaches and misuse.

04

### Legal Penalties

Organizations failing to protect customer data may face fines or lawsuits after a phishing incident.

05

### Operational disruption

Phishing can cause downtime, interrupting services and productivity while businesses recover from attacks.

06

### Identity Theft

Victims of phishing risk identity theft, allowing attackers to impersonate them for illegal activities.

# 6 THINGS TO REMEMBER IN ORDER TO PREVENT PHISHING

---

**Preventing Email Phishing**

Use email filters to block suspicious messages and implement multi-factor authentication (MFA). Learn to recognize scammer tactics and always verify sender identities before clicking links or downloading attachments. If facing potential bank or financial scams, contact your bank directly to confirm the legitimacy of communications.

**Preventing failing victim to Cloned Websites**

Always verify URLs before entering login details and use tools like www.urlvoid.com to detect fake websites. Install anti-phishing toolbars and extensions, and regularly update your browser security settings. Remember, credit cards are payment instruments; you cannot receive money on them. Never submit credit card details through suspicious links to receive funds.

**Preventing Smishing and Vishing**

Verify requests by calling the official number of organizations or relatives directly. Never share personal information unless you initiated contact. Use call-blocking apps to reduce spam and avoid responding to unknown numbers. Do not share sensitive details via phone; contact companies through verified numbers or websites. Block suspicious numbers immediately.

# 6 THINGS TO REMEMBER IN ORDER TO PREVENT PHISHING

---

### Preventing e-commerce Phishing

To prevent eCommerce phishing scams, avoid communicating outside the platform after posting a sale. Stick to official messaging systems and never share personal details through external channels. Verify buyer identities and be cautious of offers that seem too good to be true. Report suspicious messages immediately.

### Data Privacy is your best friend

Data privacy is crucial in today's digital world. Protecting your personal information helps prevent identity theft, financial loss, and unauthorized access to your accounts. Prioritizing data privacy ensures your sensitive information remains confidential and secure. Use unique, strong passwords and Password Managers.

### Report the Phishing attempts

If you suspect a phishing attempt, report it to your organization's IT department or a cybersecurity platform to help prevent others from becoming victims.

# Be smarter than the average angler

Staying informed and utilizing the right tools are key components in defending against phishing attacks.
By regularly educating yourself and leveraging these recommended solutions, you can significantly reduce your risk of falling victim to phishing scams. Stay vigilant, and keep your digital environment secure.

# Who Am I?

I am Brîndușa, Senior Test Analyst. Over the years I prevented thousands of bugs from reaching Production. I bring 15 years of sharp attention to detail and a user-focused mindset to every project.

In my free time, I enjoy traveling to destinations filled with history and amazing food. My love for exploring diverse cultures and cuisines inspires me to bring a fresh perspective to my work, enabling me to tackle even the most difficult to find defects with creativity and an open mind.

Find me on **Linkedin** and on my own **Website**