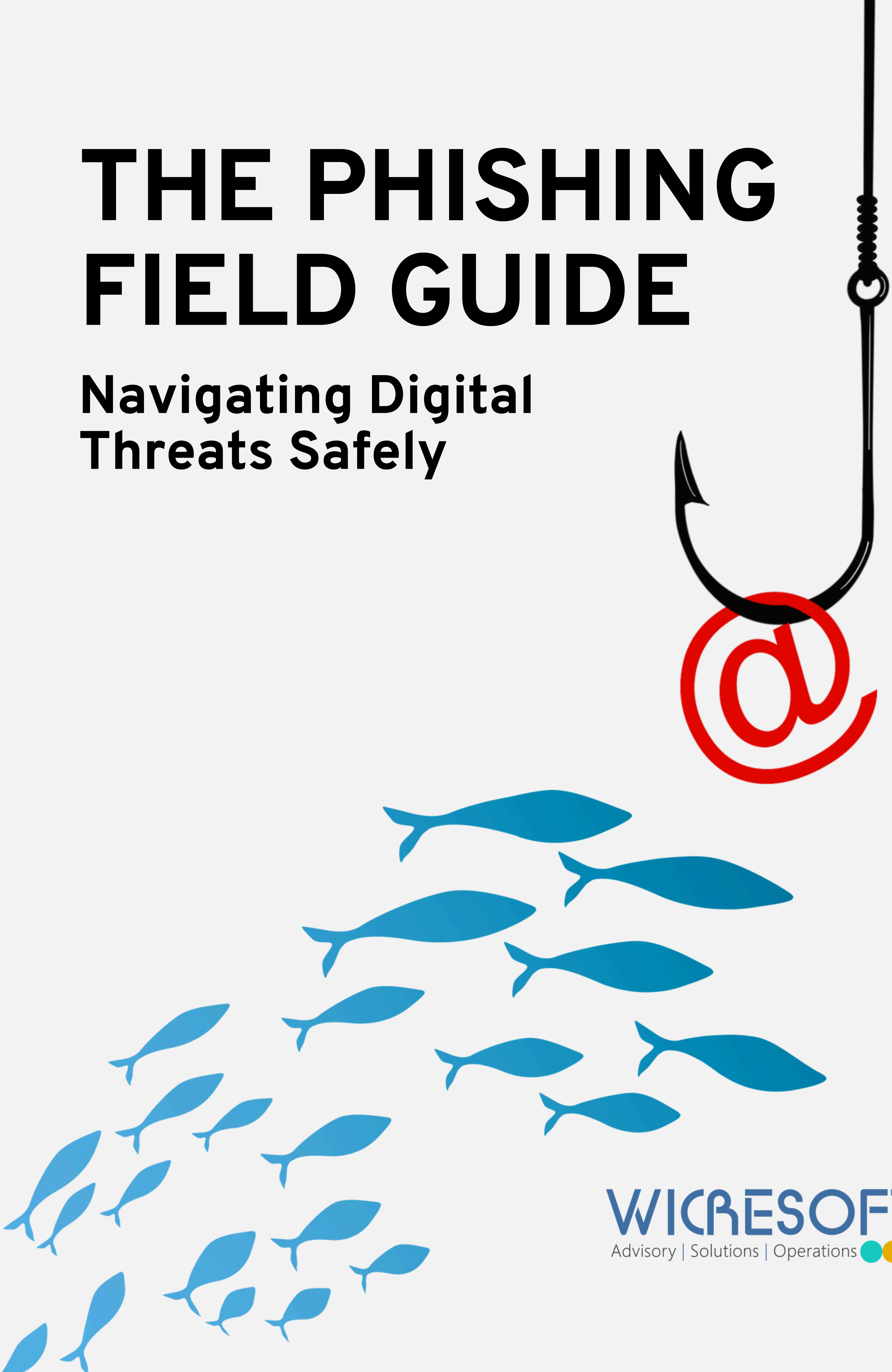
THE PHISHING FIELD GUIDE

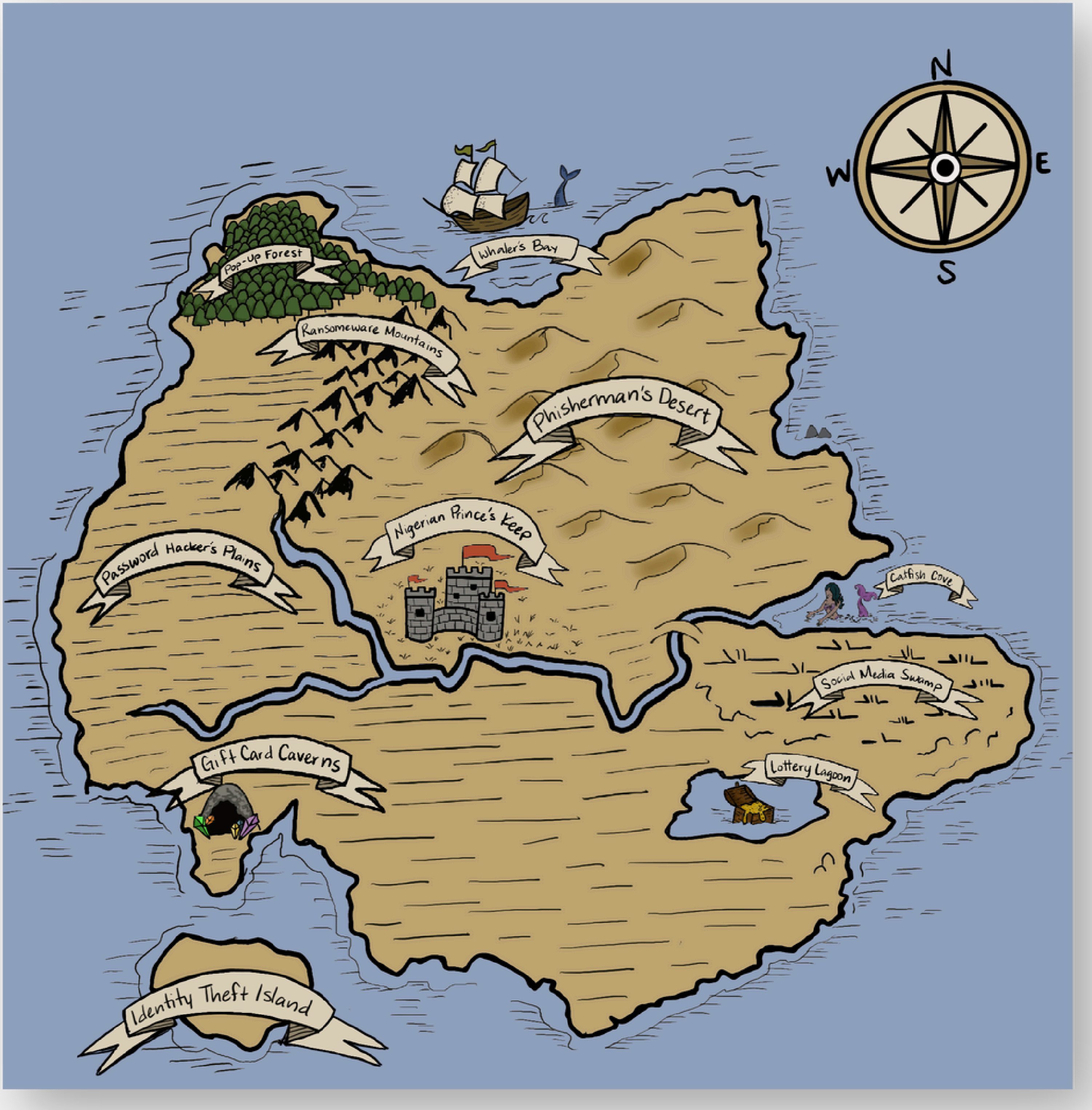
Navigating Digital Threats Safely



WICRESOFT

Advisory | Solutions | Operations

There are all kinds of digital phishing threats out there. In this map, you may see some familiar culprits. Can you navigate Cyber Island safely?



In the vast expanse of our digital oceans, we find ourselves akin to fish navigating the complex waters, teeming with both opportunity and danger. As fish must be ever vigilant of the predators lurking below, we too must be cautious of the sophisticated tactics employed by phishers seeking to exploit our vulnerabilities.

The waters of the internet are deep and wide, and within them, various phishing strategies have evolved. These strategies, tailored to exploit specific vulnerabilities, are designed with one goal in mind: to ensnare the unsuspecting. However, by understanding the nature of the threats we face, we empower ourselves to navigate with confidence and security.

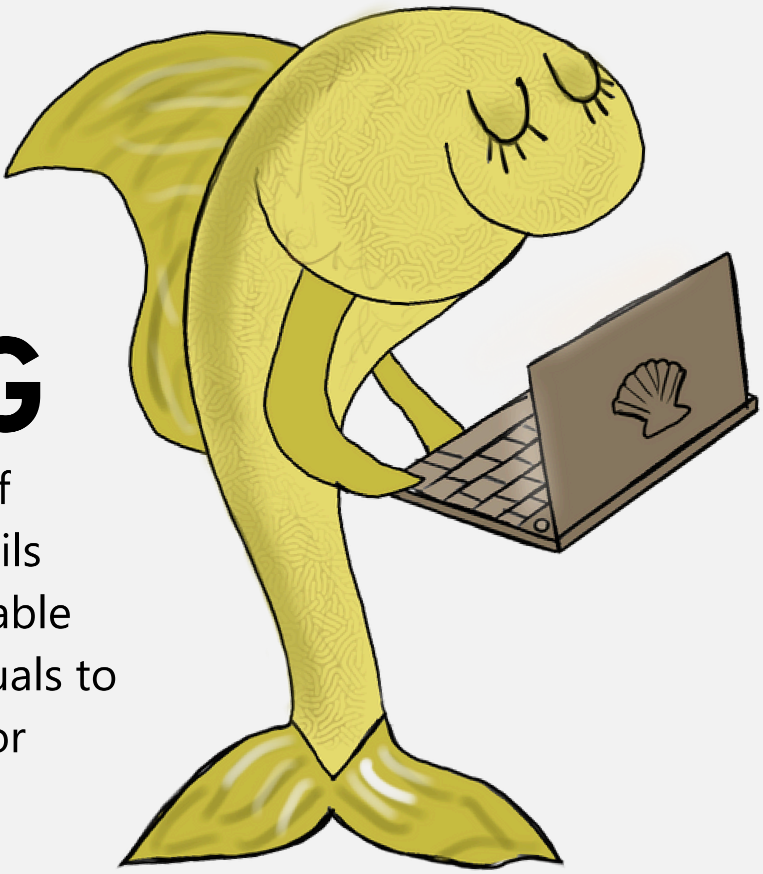
This guide offers a comprehensive overview from our perspective – that of the 'fish' – to arm you with the knowledge to recognize and evade the predatory tactics of phishers. Here's what we'll cover:

1. Common phishing tactics
2. What to look for to recognize these attacks
3. How to protect yourself from these threats

By becoming well-versed in the strategies employed by adversaries, we equip ourselves to swim safely, avoiding the lures and nets cast our way. Let this guide be your compass as you navigate the digital depths, ensuring you remain free and uncaught in these expansive waters.

EMAIL PHISHING

The most widespread form of phishing, attackers send emails pretending to be from reputable companies to induce individuals to reveal personal information or make a payment.



How to Identify

Unsolicited emails asking for personal or financial details.

Generic greetings, e.g., "Dear Customer."

Suspicious-looking email addresses.

Urgent or threatening language.

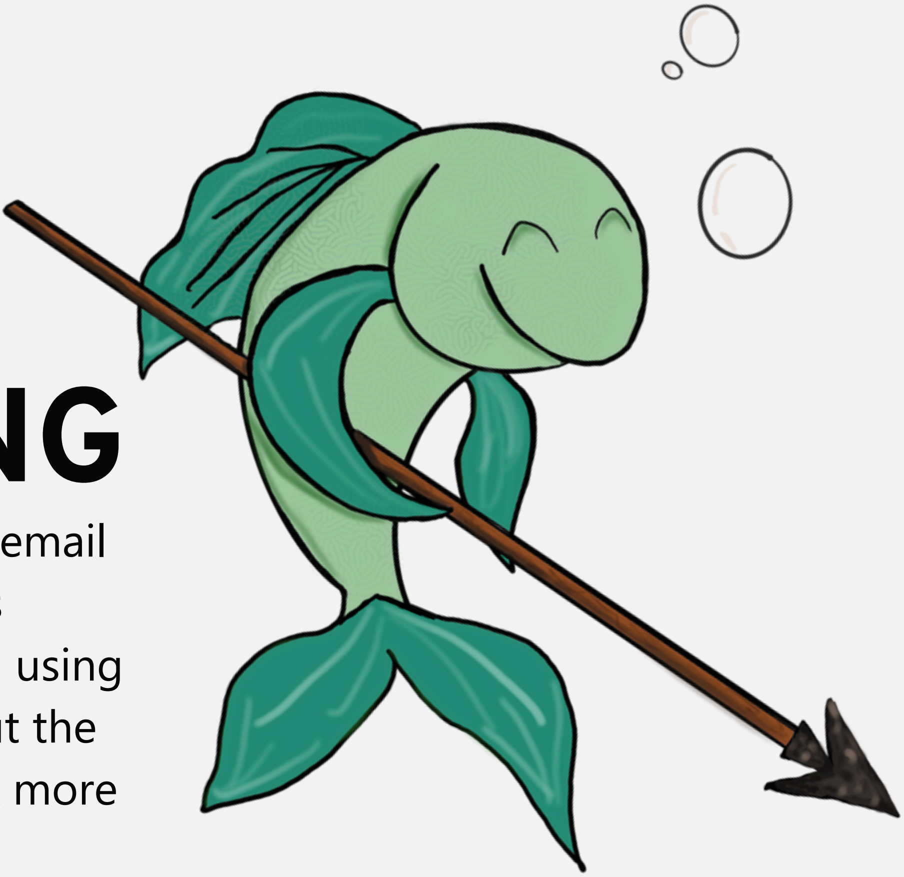
Protection Tips

Never click on links or download attachments from unknown senders.

Verify the sender's email address.

Use email filters to block spam.

SPEAR PHISHING



A more targeted form of email phishing, where attackers customize their approach using specific information about the victim to make the attack more believable.

How to Identify

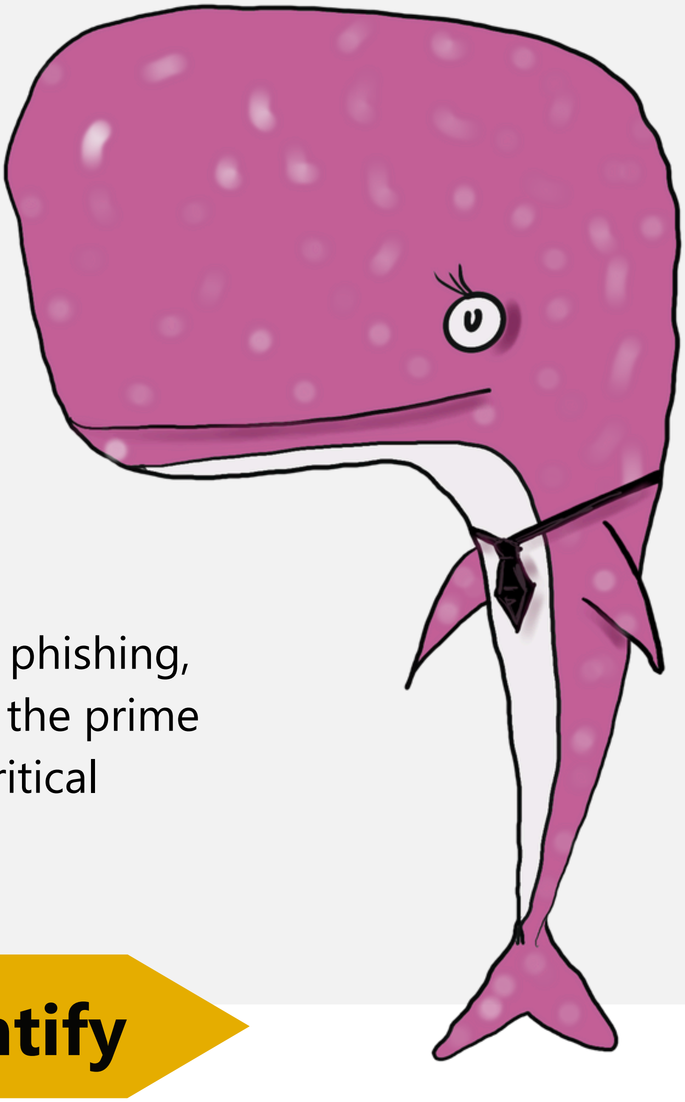
Emails from colleagues or higher-ups asking for sensitive information.

Unsolicited emails requesting a task that's out of the ordinary.

Protection Tips

Always verify unusual requests through another communication channel.

Be cautious of sharing personal details on public platforms, which can be harvested for spear phishing.



WHALING

This is a sub-category of spear phishing, where top-level executives are the prime targets, given their access to critical company data.

How to Identify

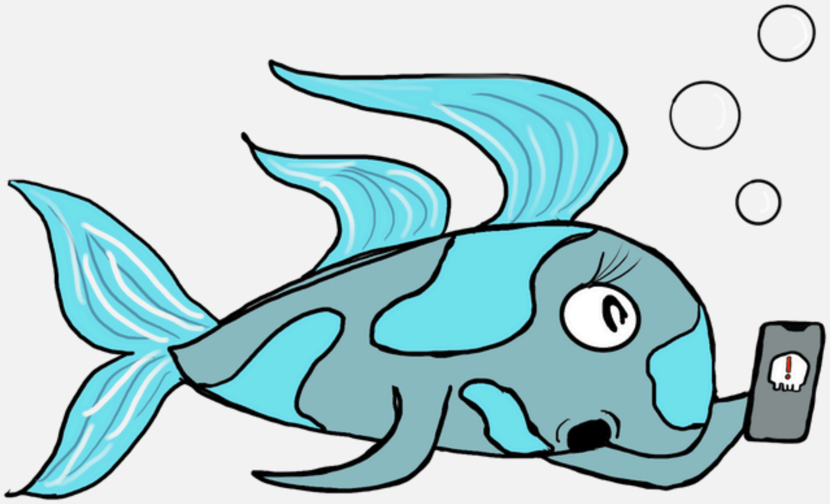
Emails requesting urgent fund transfers.

Messages that bypass regular procedures or protocols.

Protection Tips

Executives should undergo regular security training.

Implement multi-factor authentication for all financial transactions.



SMISHING (SMS PHISHING)

Phishing attempts conducted through SMS. Attackers pose as reputable entities, sending text messages to lure victims.

How to Identify

Unsolicited texts with links.

Messages conveying a sense of urgency.

Protection Tips

Don't click on links from unknown numbers.

Confirm with the purported sender through another channel before acting.

VISHING (VOICE PHISHING)

Scammers use phone calls to trick individuals into giving away sensitive information.

How to Identify

Unsolicited calls asking for personal or financial details.

Callers who rush or pressure you.

Protection Tips

Never give out personal information over the phone unless you initiated the call.

If in doubt, hang up and call the company directly using their official contact.

ANGLER PHISHING

Attackers use social media platforms to impersonate customer service accounts of well-known organizations, luring victims to fake support pages where they're asked for sensitive details.

How to Identify

Accounts without verification badges offering support.

Unsolicited DMs asking for personal or financial details.

Protection Tips

Always check for official verification badges on social media accounts.

Reach out to the company through their official website or phone number instead of responding to DMs.

QUISHING (QR CODE PHISHING)

Attackers use QR codes to direct victims to malicious websites. Often, these QR codes are distributed through emails, posters, or social media, leading unsuspecting victims to fake support pages where they're asked for sensitive details.

How to Identify

Unsolicited QR codes received through email or social media.

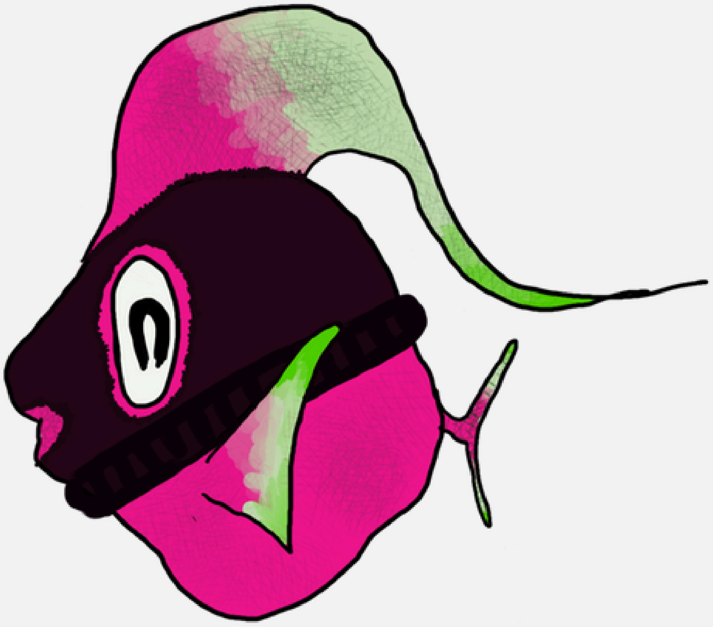
QR codes that promise rewards or urgent action without verification.

Protection Tips

Only scan QR codes from trusted sources.

Verify the URL after scanning a QR code before entering any personal information.

HTTPS PHISHING



Attackers send the victim an email with a link to a fake website that appears legitimate due to its HTTPS designation. This site is designed to trick the victim into entering their private information, leveraging the false sense of security provided by the HTTPS protocol.

How to Identify

Even if the website uses HTTPS, carefully examine the URL for subtle misspellings, extra characters, or unusual domains.

Click on the padlock icon in the browser's address bar to view the certificate details.

Protection Tips

Use MFA on all your accounts to add an extra layer of security.

Password managers can detect phishing sites when the domain does not match the saved credentials for the intended site.

Staying Safe in the Digital Ocean

The digital world, like the ocean, can be both exciting and perilous. With the right knowledge, tools, and practices, you can navigate these waters safely and confidently. Remember, phishing attacks prey on the unaware, so staying informed is your best line of defence. Here are some helpful resources:

1. National Cyber Security Centre (NCSC): Your go-to resource for the latest advice on cyber security and protection against cyber threats. Visit NCSC
2. Cyber Aware: A government-backed campaign offering actionable advice on how to bolster your online defences. Learn More
3. Action Fraud: The UK’s national fraud and cyber crime reporting centre. If you've been a victim of a cyber attack, report it here. Report Now
4. Get Safe Online: Offering practical advice on how to protect yourself, your devices, and your data. Discover Tips

What's Next?

The world of cyber security is ever-evolving, and so are the tactics of cybercriminals. Continuously educating yourself and your team is the key to staying a step ahead. Share this guide with colleagues, friends, and family to ensure they too can recognise and respond to threats.

If you come across a suspicious email, message, or call, trust your instincts and take a moment to verify. Prevention is always better than a cure. Contact Wicresoft if you have any questions or if you would like help preventing cyber attack on your business.