I. Introduction

Phishing attacks in the UK are indeed on the rise, with cybercriminals using increasingly sophisticated methods to deceive individuals and organizations into revealing sensitive information. The National Cyber Security Centre (NCSC) and other organizations like Action Fraud are actively working to combat these threats, providing resources for individuals to report suspicious activities and offering guidance on how to avoid falling victim to these scams. The 2023 Data Breach Investigations Report revealed that 74% of breaches involved the human element, which includes social engineering attacks, errors, or misuse.

Emerging scams include QR phishing, also called 'quishing', where criminals hide malicious links in QR codes. These scams often start on social media, with criminals responding to fans who posted, looking for tickets or listing fake tickets themselves.

Artificial Intelligence (AI) is also being used by cybercriminals to enhance their phishing attacks. Generative AI can be used to create well-written, personalized phishing emails, making them more convincing and effective. In addition, AI has made deepfaking, a method used to impersonate biometric authentication methods like fingerprints, facial recognition, and voice recognition, much less costly.

II. Tackling phishing in the UK

Tackling phishing in the UK involves a multi-faceted approach that includes government initiatives, collaboration with tech companies, law enforcement actions, and education and awareness programs.

The UK government has taken several steps to combat phishing and other forms of cybercrime. The National Cyber Security Centre (NCSC), a UK government organization, has the power to investigate and take down scam email addresses and websites. The government has also signed a "world-first" charter with some of the biggest technology companies, which commits these companies to blocking and removing fraudulent content from their platforms. In addition, the government has launched a new Fraud Strategy, which includes a new National Fraud Squad led by the National Crime Agency and the City of London Police.

Law enforcement agencies are also playing a crucial role in combating phishing. The National Crime Agency (NCA) is committed to improving the UK's resilience to cyber-attacks and improving the law enforcement response to the cyber-crime threat. The Metropolitan Police Cyber Crime Unit has led multi-agency and international law enforcement operations to take down facilities used by fraudsters.

Education and awareness are key to preventing phishing attacks. Various organizations offer Phishing Awareness Training Courses that educate individuals and employees about the threat posed by phishing and how to recognize and prevent such attacks. The NCSC provides guidance on how to defend against phishing attacks and how to spot and report scam emails, texts, websites, and calls.

Collaboration with international partners is also crucial in tackling phishing, especially given that many cyber threats originate from overseas. The UK's NCSC has joined forces with the National Security Agency (NSA) in the US and other international partners to release updates about ongoing threats and provide guidelines to protect against them.

III. Why phishing in the UK matters

Phishing in the UK matters because it is a significant and growing threat to individuals, businesses, and the nation's critical infrastructure. Phishing attacks, which often involve tricking people into revealing sensitive information or installing malware, have become increasingly sophisticated and prevalent. The National Cyber Security Centre (NCSC) has warned of targeted spear-phishing campaigns against UK organizations and individuals, highlighting the enduring and significant threat to the UK's critical infrastructure.

The financial impact of phishing is substantial, with businesses reporting staggering losses. For instance, in 2021, phishing attacks resulted in a loss totaling $44.2 million globally, and the average cost for an organization to recover from a data breach in the UK surpasses £3.4 million. Moreover, the UK is the biggest target for phishing attacks in Europe, with 96% of organizations in the UK being targeted by phishing.

Phishing also has a considerable impact on the public. Around nine in ten online adults in the UK have encountered content they suspected to be a scam or fraud. The psychological effects on individuals can include anxiety, stress, and other emotional disturbances, which can lead to decreased productivity and absenteeism.

A. Recent phishing attacks in UK

Phishing attacks continue to be a significant cybersecurity threat in the UK, with various recent examples demonstrating the diverse tactics used by cybercriminals.

- **Vishing Attacks from Ukraine and Czech Republic**: In November 2023, an international operation disrupted

OVERKILL SECURITY

a phishing campaign that defrauded victims of tens of millions of euros. The criminals carried out vishing (voice phishing) attacks from call centres in Ukraine, posing as bank employees to pressure victims into transferring money

- **Hotel Employee Phishing Campaign**: In the same month, phishing campaigns targeted hotel employees. The attackers sent emails to hotel employees, tricking them into clicking a malicious link that downloaded infostealer malware. Once infected, the attackers exfiltrated customer data
- **Fake USPS Emails**: In May 2023, the USPS and the Postal Inspection Service reported the circulation of fake emails/email scams claiming to be from USPS officials. These emails prompted recipients to confirm their personal delivery information by clicking a button that, when opened, could activate a virus and steal information
- **UK Transport Business Phishing Attack**: In the first quarter of 2021, a UK transport business was hit by a cyber-attack where an email with a document containing a link to a fake portal was sent to the employees of the organization. The fake portal required the recipient to log in using Office 365/G-Suite authentication credentials. When recipients logged in, their credentials and passphrases were harvested and then used to access the victims' mailboxes
- **QR Phishing**: In 2024, a new form of phishing called 'quishing' emerged, where criminals hide malicious links in QR codes. They try to get people to hand over their personal information or download malware. This type of phishing can appear as emails claiming a package hasn't been delivered or that there's a problem
- **Phishing Attack on Law Firm**: A law firm employee failed to recognize a phishing attack. They received an email, clicked a link to download a document, then inadvertently entered login credentials into what they believed was a legitimate website. This resulted in a data breach

B. *Recent phishing attacks targeting UK business*

Phishing attacks continue to be a significant threat to businesses in the UK, with several notable incidents occurring in recent years.

- **British Library Cyber Attack (January 2024)**: The British Library suffered a cyber attack that rendered its IT systems inoperable. The Rhysida ransomware gang claimed responsibility for the attack and leaked internal human resources data, including scans of employee passports and employment contracts, on the dark web
- **WhatsApp Job Offer Scam (November 2023)**: Thousands of job seekers were targeted by scammers on WhatsApp, who used fake job offers to lure victims into their scheme
- **Phishing Attacks on Small Businesses (2023)**: Research revealed that scams and phishing made up 82% of online threats for small businesses in the UK in 2023. In the first half of 2023 alone, email-based phishing attacks surged 464% in comparison to 2022
- **Phishing Attacks on UK Organizations (2022-2023)**: 83% of UK businesses and charities that suffered a cyber attack identified phishing as the attack type

C. *Recent phishing attacks targeting UK individuals*

Phishing attacks continue to be a significant cybersecurity threat in the UK, with various recent incidents highlighting the evolving tactics of cybercriminals.

- **Phishing attack on Booking.com**: In November 2023, a phishing attack targeted Booking.com. The criminals carried out vishing (voice phishing) attacks from call centres in Ukraine, posing as bank employees to pressure victims into transferring money
- **Phishing attacks on UK parliamentarians**: In December 2023, there were spear-phishing attacks targeting UK parliamentarians from multiple political parties
- **Phishing attacks impersonating government emails**: In 2022, the National Cyber Security Centre (NCSC) reported on government impersonation scams, where phishing attacks were carried out by impersonating government emails

D. *Phishing Scams Targeting Employees*

Phishing scams targeting employees, also known as Business Email Compromise (BEC) scams, often target specific roles within a company, such as executives or HR professionals, who have access to sensitive information. These scams typically involve sending emails that appear to be from a senior executive or CEO, requesting a wire transfer or payroll information. Some common employee-targeted phishing scams include:

- **Whaling attacks**: These are targeted attempts to steal sensitive information from a company by impersonating top executives like CEOs or CFOs
- **W-2 phishing scam**: In this scam, the attacker impersonates an executive or organization leader and sends a message to a payroll or HR employee asking for W-2 information
- **New employee phishing**: New employees are often targeted because they are eager to impress and may overlook subtle signs of a phishing attack

E. *Phishing Scams Targeting Consumers*

Phishing scams targeting consumers often impersonate well-known companies or organizations, such as banks or government agencies, to gain the trust of the targeted individuals. These scams typically involve sending emails or text messages that appear to be from these entities, asking consumers to provide personal identifying information. The scammers then use this information to commit fraud, such as opening new accounts in the consumer's name or invading their existing accounts. Some common consumer-targeted phishing scams include:

- **The check-cashing scam**: Scammers target people selling items online. They overpay with a check and ask for the excess to be wired back, only for the original check to bounce

OVERKILL SECURITY

- **The sales scam**: Online shoppers looking for a bargain are targeted on auction sites with high-end electronics. Even if the consumer doesn't win the item, they still have to pay

- **The job scam**: An apparent employer conducts a phone interview and tells a job seeker they have received a job. The job seeker is then asked to fill out an online credit form, which is used to steal their identity

IV. STRATEGIES TO GET AHEAD OF PHISHING

Phishing is a significant cybersecurity threat, and early detection is crucial to prevent victims from falling prey to these attacks.

- **Detect Phishing Early and Often**: Early detection of phishing attacks is vital as 50% of victims fall prey to a phishing attack within 24 hours. Leveraging technology and automation can help identify phishing pages earlier. Deep learning models combined with browser automation can be used to build an automated solution for early detection

- **Use DMARC**: Domain-based Message Authentication, Reporting, and Conformance (DMARC) is a global standard for email authentication that helps verify the origin of emails and block out fake emails. It allows senders to verify that the email really comes from whom it claims to come from, helping curb spam and phishing attacks

- **Monitor Domain Registrations**: Monitoring domain registrations can help detect fraudulent websites set up to steal login credentials, divert web traffic, or sell counterfeit products. Services like PhishLabs and Red Points offer domain monitoring services that can automate the process of finding and removing fake accounts, apps, websites, and domains

- **Automate Phishing Detection**: Machine learning can help detect phishing attacks by learning patterns and creating models that can automatically distinguish between legitimate and malicious websites or other forms of communication. There are also various anti-phishing tools and services available that can help businesses protect against phishing attacks

- **Collaborate Across Teams**: Collaboration across teams is essential in combating phishing. Regular staff awareness training can ensure that employees know how to spot a phishing email, even as fraudsters' techniques become increasingly more advanced

A. Detect Phishing Early and Often

Early detection of phishing is critical because the first 24 hours are when victims are most susceptible. To detect phishing early and often, organizations can employ various technologies:

- **Automated Scanning**: Use automated scanning tools to regularly search for phishing websites and emails. These tools can scan and analyze web pages, emails, and other digital content for phishing indicators.

- **Machine Learning**: Implement machine learning algorithms that can learn from patterns of known phishing attacks and predict new ones. These algorithms can process large volumes of data to identify potential threats more quickly than humans.

- **User Reporting**: Encourage users to report suspected phishing attempts. Quick reporting can lead to faster takedown of phishing sites and prevent further damage.

B. Use DMARC

Domain-based Message Authentication, Reporting, and Conformance (DMARC) is an email-validation system designed to protect domain names from being used in phishing scams, email spoofing, and other cybercrimes:

- **Email Authentication**: DMARC works by ensuring that legitimate email is properly authenticated against established DKIM (DomainKeys Identified Mail) and SPF (Sender Policy Framework) standards.

- **Reporting**: DMARC also provides a way for email receivers to report back to senders about messages that pass and/or fail DMARC evaluation.

- **Policy Enforcement**: Senders can set policies for how receivers should handle mail that doesn't pass authentication checks, potentially preventing delivery of fraudulent emails.

C. Monitor Domain Registrations

Monitoring domain registrations can help identify potential phishing sites before they become active:

- **Domain Watch Services**: Use services that monitor domain name registrations for names that are similar to your brand or trademarks.

- **Automated Alerts**: Set up automated alerts to notify your security team when a potentially fraudulent domain is registered.

- **Take-down Services**: Engage with take-down services that can help remove phishing sites once they are identified.

D. Automate Phishing Detection

Automation in phishing detection involves using software to identify and respond to phishing threats:

- **Phishing Databases**: Utilize databases of known phishing sites to block access to them.

- **Real-time Analysis**: Implement systems that perform real-time analysis of web pages and emails to detect phishing content.

- **Integration**: Integrate phishing detection into security infrastructure like firewalls, email gateways, and endpoint protection for a comprehensive defense.

E. Collaborate Across Teams

Collaboration is key to a successful anti-phishing strategy:

- **Cross-departmental Training**: Conduct regular training sessions across all departments to educate employees about the latest phishing tactics and how to recognize them.

OVERSILL SECURITY

- **Shared Intelligence**: Share intelligence about new phishing threats between security teams, IT departments, and other relevant stakeholders.
- **Incident Response Planning**: Develop and practice an incident response plan that involves multiple teams to ensure a coordinated response to phishing attacks.

V. PHISHING DETECTION AND RESPONSE SOFTWARE

Phishing detection and response software is a set of cybersecurity tools that allow organizations to identify and remediate phishing threats. Here are some tools that can be used to automate phishing detection:

- **Agari Phishing Response**: This service is a phishing incident response system designed to accelerate phishing triage, forensics, remediation, and breach containment
- **IRONSCALES**: This self-learning email security platform is designed to proactively fight phishing. It combines human interaction and AI-oriented identification to prevent phishing attempts, including Business Email Compromise (BEC)
- **Avanan**: This anti-phishing software for cloud-hosted email ties into your email provider using APIs to train their AI using historical email. The service analyzes not just message contents, formatting, and header information, but evaluates existing relationships between senders and receivers to establish a level of trust
- **Barracuda Sentinel**: This tool leverages mail provider APIs to protect against phishing. It uses artificial intelligence to learn the unique communications patterns of your organization to identify and block real-time spear phishing and cyber fraud attacks
- **Proofpoint Targeted Attack Protection (TAP)**: This tool helps organizations efficiently detect, mitigate, and block advanced targeted attacks that arrive via email
- **RSA FraudAction**: This tool specializes in detecting and preventing phishing attempts, Trojans, and rogue websites
- **PhishER**: This lightweight Security Orchestration, Automation, and Response (SOAR) platform helps orchestrate threat response and manage the high volume of phishing threats
- **Zphisher**: This is a phishing tool for beginners and novices, which includes some automated phishing tests
- **Evilginx2**: This phishing tool describes itself as a man-in-the-middle attack framework used for phishing login credentials along with session cookies, allowing bypass of 2-factor authentication
- **DTonomy AIR Enterprise**: This AI-based tool includes batch mode analysis of phishing emails, task and case management automation, and hundreds of playbooks

A. *Key Features in Phishing Detection and Response Software*

When selecting phishing detection and response software, consider the following key features:

- **Domain Identification**: The ability to identify and verify the authenticity of the domain from which an email originates, helping to prevent domain spoofing
- **Header Analysis**: Analyzing email headers for inconsistencies or signs of tampering that may indicate a phishing attempt
- **Link Analysis**: Examining links within emails or web content to determine if they lead to known phishing sites or malicious content
- **Attempted Impersonation Features**: Detecting attempts to impersonate legitimate entities or individuals, which is a common tactic in spear-phishing attacks
- **AI Analytics**: Using artificial intelligence to proactively identify suspicious behavior patterns and predict new phishing threats
- **Cross-referencing with Threat Libraries**: Comparing against databases of known threats, which are often manually updated by security experts, to identify phishing attempts
- **End-user Reporting**: Enabling users to report suspected phishing attempts, which can lead to faster takedown of phishing sites and prevent further damage

B. *How Phishing Simulation and Testing Tools Work*

Phishing simulation and testing tools are designed to give users real-world experience in combating phishing attacks:

- **Realistic Simulations**: Distribute a range of realistic phishing scenarios that mimic the latest attack methods, including vishing (voice phishing), to train users
- **Regularly Updated Templates**: Use templates that are frequently updated to reflect the latest phishing tactics, ensuring that training remains relevant
- **Automated Testing Frequency**: Automate the frequency of phishing simulation tests to ensure consistent training rather than sporadic, one-off sessions
- **Active Environment Testing**: By seeing a phishing email in an active environment, users must apply their knowledge to prevent becoming a victim, reinforcing their training
- **Admin Insights**: From an admin perspective, deploying simulations and training provides insight into the effectiveness of the training and the organization's security posture

C. *Implementing phishing detection and response software*

Implementing phishing detection and response software effectively requires a combination of technical solutions, user education, and organizational policies:

- **Regular Employee Training in Cybersecurity Awareness**: Continuous training ensures that

OVERKILL SECURITY

employees can recognize and respond to phishing attempts. Engaging training platforms can keep employees updated on the latest phishing tactics

- **Implement Email Security Best Practices**: Utilize protocols like DMARC (Domain-based Message Authentication, Reporting, and Conformance) to authenticate emails and prevent spoofing. This protocol builds on SPF and DKIM standards to verify the origin of emails and block fake ones
- **Leverage AI and Automation**: AI-powered software can scan incoming messages for signs of phishing with high accuracy. Machine learning algorithms can also predict new phishing threats by learning from patterns of known attacks
- **Monitor Phishing Results**: Use phishing simulation tools to monitor employee responses to simulated attacks. This can help identify vulnerabilities and measure the effectiveness of training programs
- **Filter DNS Traffic**: DNS filtering solutions can prevent users from accessing malicious websites by blocking requests to blacklisted domains. Some filters can proactively evaluate websites for harmful code and add them to the blacklist
- **Use Technical Solutions**: Implement strong passwords, employ DNS filtering, set up antivirus solutions, enable safe web browsing policies, and use secure email services to prevent phishing compromises
- **Implement Incident Response and Reporting Measures**: Have a plan in place for responding to identified phishing activity. This includes remediation steps and reporting mechanisms to address and mitigate the impact of successful attacks
- **Secure Email Gateway Capabilities**: Deploy email filters that screen based on headers and malicious content, categorize email, and inspect URLs against reputation feeds
- **Harden User Endpoints**: Ensure that user endpoints are secure by implementing endpoint protections and educating users on safe browsing and email practices

D. *Implementation mistakes*

When implementing phishing detection and response software, there are several common mistakes to avoid:

- **Not updating software regularly**: Regular updates are crucial to ensure that the software can effectively detect and respond to the latest phishing threats
- **Over-reliance on IT departments**: While IT departments play a crucial role in managing and maintaining phishing detection software, it's important for all employees to understand how to identify and respond to phishing attempts
- **Relying on antivirus software alone**: While antivirus software can help detect and prevent some phishing attempts, it's not sufficient on its own. Endpoint detection and response (EDR) and extended detection and response (XDR) solutions can provide more comprehensive protection
- **Not conducting thoughtful phishing simulations**: Phishing simulations can be a useful tool for training employees to recognize and respond to phishing attempts. However, it's important to conduct these simulations thoughtfully and to communicate clearly with all relevant stakeholders
- **Not taking a defense-in-depth strategy**: Relying solely on an anti-phishing program can be risky, as it only takes one mistake for an attacker to succeed. A defense-in-depth strategy, which includes multiple layers of security, can provide more robust protection

When selecting phishing detection and response software, consider the following key factors:

- **Integration with other tools**: The software should be able to integrate with other security tools for a comprehensive security approach
- **Machine learning capabilities**: Many modern tools use machine learning to analyze endpoint and network activities and detect potential threats
- **Threat prioritization**: The software should be able to prioritize threat alerts to help your team focus on the most serious threats first
- **Agent vs. agentless monitoring**: Both agent-based and agentless monitoring have their pros and cons, and you may need a combination of both for optimal security
- **Monitoring and analysis capabilities**: The software should be able to monitor endpoint behaviors and detect, prioritize, track, and alert on indicators of compromise (IOCs) and indicators of attack (IOAs)

  Detection vs. prevention: Some solutions focus more on detecting phishing attempts, while others focus more on preventing them
- **Automated real-time threat detection**: This feature can help your security team quickly identify and respond to threats

VI. HOLIDAY PHISHING RISKS

A. *Why Scammers Love the Holidays*

Scammers love the holiday season for several reasons:

- **Increased Online Activity**: During the holidays, people are more active online, shopping for gifts, booking travel, and donating to charities. This increased activity provides more opportunities for scammers to trick people into revealing sensitive information
- **Distraction**: The holiday season is a busy time, and people are often distracted and may not be as vigilant as they usually are. Scammers take advantage of this by sending phishing emails that appear to be from reputable sources, such as banks or popular retailers
- **Emotional Manipulation**: Scammers often use emotional manipulation during the holiday season. They may impersonate charities or family members to trick people into sending money or revealing personal information

OVERKILL SECURITY

- **Seasonal Themes**: Scammers use holiday-themed emails, messages, and websites to trick victims. They may send fake order and tracking emails, charity emails, and messages related to holiday events or schedules
- **Opportunistic Behavior**: Scammers take advantage of the fact that many companies offer bonuses or seasonal jobs during the holidays. They create phishing campaigns that target employees with fake bonus offerings or job seekers with fraudulent job ads
- **Social Engineering**: Scammers use social engineering tactics to create a sense of urgency or fear, such as claiming that a package delivery was missed or that a recipient's account has been hacked. This can prompt hasty actions like clicking on malicious links
- **Fake Online Stores or "Lookalike Stores"**: Scammers create fraudulent websites that mimic legitimate online retailers to trick consumers into entering their personal and financial information
- **Missed Delivery/Non-Delivery Notification**: Victims receive notifications claiming a delivery was missed or a package was not delivered, prompting them to click on a link that could lead to a phishing site or install malware
- **Gift Card Scams**: Scammers send spoofed emails or texts asking victims to purchase multiple gift cards for personal or business reasons, often pretending to be someone the victim knows
- **Fake Charities**: Criminals set up bogus charities and solicit donations from individuals who believe they are contributing to a legitimate cause
- **Social Media Scams**: Scammers use social media platforms to offer holiday promotions, vouchers, or gift cards that require completing surveys designed to steal personal information
- **Fraudulent Seasonal Jobs**: Fake job ads are posted online offering good money for very little work, targeting individuals seeking to make extra money during the holidays
- **Phishing Emails**: These are particularly prevalent during the holiday season and can take the form of bogus delivery confirmation requests or other communications seeking personal information
- **Package Theft**: Scammers may pose as delivery services and send fraudulent notifications about package theft or delivery issues to trick recipients into providing personal details
- **Vacation Scams**: Offers for fake holiday vacations or travel deals that aim to steal money or personal information from unsuspecting victims
- **Brushing Scams**: Unsolicited items are sent to individuals, which may seem harmless but could be a sign that the scammer has access to the recipient's personal information

OVERKILL SECURITY