JOURNAL OF MULTIDISCIPLINARY RESEARCH AND INTEGRATED SCIENCES

**Volume 1, Issue 1, 2021** | **Article ID:** JMRIS-2021-001 | **Pages:** 1-7 | **Article Type:** Review Article
**Received:** 25 February 2021 | **Revised:** 22 March 2021 | **Accepted:** 03 April 2021 | **Published:** 15 April 2021

# Phishing and Credential-Based Cybersecurity Threats Among Remote Employees During the COVID-19 Pandemic in the United Kingdom

**Mr. Asif Irshad**[1,*]

[1] *University of South Asia, Lahore, Pakistan*

***Corresponding author:** Mr. Asif Irshad, University of South Asia, Lahore, Pakistan | Asif.irshad3056@gmail.com

## ABSTRACT

The rapid transition to remote working during the COVID-19 pandemic substantially altered the cybersecurity exposure of organisations and employees. In the United Kingdom, employees increasingly depended on email, cloud applications, virtual private networks, remote-access platforms and digital collaboration systems for routine organisational activities. These changes expanded opportunities for phishing and credential-based attacks by increasing dependence on electronic communication while reducing face-to-face verification and conventional workplace security oversight. This paper examines phishing and credential-related threats affecting remote employees during the pandemic through a structured review of literature published between 2016 and 2020. Particular attention is given to social engineering, credential harvesting, employee susceptibility, time pressure, security awareness, organisational culture and remote authentication. The review demonstrates that phishing risk cannot be adequately explained by technical vulnerabilities alone. Attack success is influenced by the interaction between persuasive message characteristics, employee cognitive processes, organisational security practices and authentication architecture. A layered cybersecurity framework is proposed for UK organisations incorporating stronger identity controls, email protection, endpoint security, contextual security-awareness interventions and rapid incident reporting. The findings emphasise that effective protection of remote employees requires simultaneous technological and human-centred measures rather than reliance on conventional awareness training or perimeter security alone.

**Keywords:** phishing; credential theft; cybersecurity; remote working; COVID-19; social engineering; information security; United Kingdom

## 1. Introduction

Phishing remains one of the most persistent mechanisms through which attackers obtain authentication credentials, initiate malware infection and gain unauthorised access to organisational information systems. Unlike attacks dependent exclusively on software vulnerabilities, phishing exploits interactions between technological systems and human decision-making. A phishing communication may imitate a legitimate institution, colleague or information service and encourage the recipient to disclose credentials, follow a malicious link or perform another security-sensitive action. Reviews of phishing techniques demonstrate that attackers combine technical deception with social-engineering principles to increase message credibility and manipulate user behaviour (Aleroud and Zhou, 2017; Mouton, Leenen and Venter, 2016).

The COVID-19 pandemic created an unusually favourable environment for such attacks. Organisations rapidly digitised processes that had previously occurred within controlled workplaces, while employees became increasingly dependent on remote communication and cloud services. Research published during 2020 identified the pandemic as a major accelerator of organisational digital transformation and highlighted the operational difficulties associated with rapidly changing information-technology practices (De, Pandey and Pal, 2020; Papagiannidis, Harris and Morton, 2020).

For organisations in the United Kingdom, this transformation meant that security controls designed around office environments increasingly had to protect users working from homes and other remote settings. Phishing therefore became particularly important because attackers did not necessarily need to compromise corporate infrastructure directly: compromising an employee's password or authenticated session could provide an alternative entry point.

This paper examines how pandemic-driven remote working intensified phishing and credential-based cybersecurity threats among UK employees and how these threats could be mitigated using integrated technical, behavioural and organisational controls. Rather than claiming new nationally representative empirical observations, the study synthesises cybersecurity evidence available by the end of 2020 and applies it specifically to the UK remote-working environment.

## 2. Review Approach

A structured narrative review was adopted to integrate technical cybersecurity research with human-factor and information-security behaviour literature. To preserve the historical perspective of a paper prepared in 2021, eligible literature was restricted to publications from 2016 to 2020. The review concentrated on studies addressing phishing, social engineering, information-security awareness, policy compliance, credential security, cybersecurity behaviour, organisational security culture and pandemic-related digital transformation.

Particular emphasis was placed on articles published in high-ranking information-systems, cybersecurity and human-computer-interaction journals. The synthesis was organised around four interacting dimensions: attack characteristics, employee susceptibility, remote-working conditions and organisational controls. The approach is intentionally analytical rather than meta-analytic because the included studies employ heterogeneous experimental, behavioural, organisational and conceptual methodologies.

## 3. Phishing and Credential Threats in the Remote-Working Environment

### 3.1 Expansion of the attack surface

Remote working changes the environment in which security decisions are made. Employees may alternate between organisational and personal devices, use home networks, authenticate repeatedly to cloud platforms and receive a greater proportion of organisational communication electronically. Consequently, an unexpected authentication request can become more difficult to distinguish from a legitimate workflow.

Phishing attackers exploit precisely this ambiguity. Aleroud and Zhou (2017) demonstrate that phishing encompasses multiple technical and social mechanisms, while Goel and Jain (2018) show that mobile environments introduce additional difficulties because restricted screen dimensions and interface characteristics can obscure indicators that help users evaluate legitimacy.

Credential phishing is particularly consequential in remote environments because passwords frequently operate as gateways to interconnected services. A successful imitation of a cloud sign-in page, webmail portal, virtual private network or collaboration platform can therefore transform a single human error into unauthorised access to multiple organisational resources.

### 3.2 Contextual social engineering

Social engineering is successful partly because communications are designed to correspond with recipients' expectations. During a disruptive event, attackers can construct believable messages around urgent organisational announcements, health information, remote-access changes, password resets or collaboration requests.

Social-engineering scenarios documented before the pandemic already demonstrated the importance of authority, urgency, familiarity and contextual credibility (Mouton, Leenen and Venter, 2016). Research on phishing susceptibility similarly indicates that individuals differ in their response to social influence and message characteristics (Parsons et al., 2019).

The pandemic did not therefore create an entirely new category of cyberattack. Rather, it produced a highly effective context for established attack mechanisms.

### 3.3 Time pressure and disrupted decision-making

Remote employees frequently interact with messages while simultaneously managing meetings, family interruptions, multiple communication channels and unfamiliar technical processes. Such conditions are important because cybersecurity decisions are not made under ideal cognitive circumstances.

Chowdhury, Adam and Teubner (2020) identify time pressure as an important component of human cybersecurity behaviour and argue that rushed decision environments can negatively affect security decisions. Consequently, phishing defences that assume employees will carefully inspect every URL, sender address and authentication prompt are inherently limited.

*The conceptual pathway from pandemic disruption to credential compromise is presented in Figure 1.*

Figure 1 interpretation: Pandemic disruption acts primarily as a threat multiplier. It modifies technological routines and employee decision contexts, thereby increasing opportunities for existing phishing mechanisms.

## 4. Human Factors and Organisational Vulnerability

### 4.1 Security awareness is necessary but insufficient

Awareness influences security behaviour, but awareness cannot be equated with perfect resistance to phishing. Employees may understand that phishing exists while still responding incorrectly to a convincing message. Information-security awareness instruments such as the HAIS-Q illustrate that security behaviour involves knowledge, attitudes and behavioural practices rather than simple recognition of security terminology (Parsons et al., 2017).

Li et al. (2019) further demonstrate that awareness of cybersecurity policies is associated with employee cybersecurity behaviour, suggesting that policies must be understood and internalised rather than merely distributed.

For remote organisations, annual generic cybersecurity training is therefore unlikely to be sufficient. Training must be reinforced within the employee's actual digital workflow.

### 4.2 Organisational culture and shared responsibility

Security behaviour also occurs within a social environment. Employees observe colleagues, respond to managerial expectations and interpret whether security procedures are genuinely valued. Da Veiga et al. (2020) conceptualise information-security culture as an organisational phenomenon rather than an exclusively individual responsibility, while Wiley, McCormac and Calic (2020) demonstrate relationships between cultural characteristics and information-security awareness.

This is particularly important when employees are physically separated. Informal opportunities to ask a colleague whether an email is genuine are reduced, while fear of appearing incompetent may discourage employees from reporting suspicious interactions.

### 4.3 Previous experience does not guarantee immunity

Repeated exposure can improve recognition, but previous phishing experience does not automatically eliminate future susceptibility. Chen, Gaia and Rao (2020) examined how recent phishing encounters influence subsequent susceptibility, highlighting the dynamic nature of phishing decision-making rather than treating vulnerability as a fixed employee characteristic.

Security programmes should therefore avoid dividing employees simplistically into "safe" and "unsafe" groups. Risk changes according to message content, task context and situational pressure.

*The principal phishing and credential-security risks and the corresponding organisational controls are summarised in Table 1.*

## 5. A Layered Defence Strategy for UK Organisations

The evidence indicates that phishing cannot be controlled by asking employees simply to "be more careful". The appropriate response is defence in depth, in which failure at one layer does not automatically result in account compromise.

### 5.1 Strengthening identity and authentication

Organisations should reduce their dependence on passwords as a single point of failure. Multi-factor authentication can ensure that possession of a stolen password alone is insufficient for successful authentication. Centralised identity management can additionally support conditional access based on device status, location, login characteristics or other risk indicators.

Authentication controls should nevertheless be designed to minimise unnecessary prompts. Excessive security prompts can become habitual and may encourage users to approve requests without appropriate scrutiny.

### 5.2 Email and communication security

Technical filtering should identify spoofing, malicious domains, suspicious URLs and dangerous attachments before messages reach employees. However, phishing evolves in response to filtering technology, meaning that preventive controls must be complemented by detection and response mechanisms.

Sensitive requests should also have explicit verification procedures. For example, password resets, financial changes and requests for confidential information should not depend exclusively on the authenticity of a single email.

### 5.3 Human-centred security training

Training should reproduce the situations employees actually encounter. Research on security-awareness programmes shows that organisational interventions can influence policy compliance, while phishing research demonstrates that susceptibility is shaped by context rather than knowledge alone (Bauer, Bernroider and Chudzikowski, 2017; Parsons et al., 2019).

For UK organisations operating remotely, simulations should therefore include plausible cloud-login notifications, IT-support messages, collaboration invitations and managerial requests. Employees should immediately receive constructive feedback explaining which indicators were suspicious and what action should have been taken.

### 5.4 Security culture and incident reporting

Alshaikh (2020) argues for the development of cybersecurity culture capable of influencing employee behaviour rather than treating security as an isolated technical activity. Remote employees should consequently be provided with a highly visible, low-friction mechanism for reporting suspicious communications.

A constructive reporting culture is crucial. An employee who realises that credentials may have been disclosed should report the incident immediately rather than attempting to conceal the mistake. Rapid reporting allows password reset, session revocation, account investigation and containment before an attacker can expand access.

*The proposed layered defence model for remote-worker phishing and credential threats is presented in Figure 2.*

Figure 2 interpretation: Protection should be constructed so that the compromise of a single layer—particularly human recognition—does not provide unrestricted organisational access.

## 6. Discussion

The central implication of the reviewed literature is that pandemic-era phishing should be understood as a socio-technical cybersecurity problem. Remote working simultaneously changed the technical infrastructure through which employees accessed organisational resources and the psychological environment in which authentication decisions were made.

Traditional organisational cybersecurity frequently assumes a definable network perimeter. Remote work weakens the usefulness of this assumption because users, endpoints, networks and cloud services operate across multiple environments. Consequently, identity increasingly becomes a central security boundary. From an attacker's perspective, obtaining a legitimate employee credential may be more efficient than attempting to exploit hardened organisational infrastructure directly.

However, technological controls alone cannot eliminate risk. Social-engineering attacks deliberately exploit normal human characteristics including trust, responsiveness to authority and the desire to complete tasks efficiently. Organisational policies that conflict substantially with ordinary work practices may even encourage insecure workarounds. Studies of security-policy compliance repeatedly demonstrate that organisational and behavioural factors influence whether employees follow prescribed security practices (Safa, Von Solms and Furnell, 2016; Rajab and Eydgahi, 2019).

The appropriate objective is therefore not an unrealistic expectation of perfect employee detection. UK organisations should instead design systems under the assumption that some phishing messages will bypass technical filtering and some employees will eventually interact with them. Security architecture should minimise both the probability and consequences of that interaction.

This approach also changes the measurement of cybersecurity performance. Training completion rates alone are weak indicators of resilience. More meaningful measures include simulated-phishing reporting rates, time between suspicious activity and reporting, proportion of accounts protected by strong authentication, frequency of unsafe credential reuse, and the speed with which compromised sessions can be revoked.

## 7. Conclusion

The COVID-19 pandemic intensified conditions favourable to phishing and credential-based cybersecurity attacks by accelerating remote working, digital communication and cloud authentication. For remote employees in the United Kingdom, the resulting threat cannot be attributed solely to either technological vulnerabilities or individual negligence. Phishing operates through the interaction of persuasive attack design, employee decision-making, security culture and identity infrastructure.

Evidence available between 2016 and 2020 shows that awareness, policy compliance, organisational culture, time pressure and social influence all affect cybersecurity behaviour. The most effective organisational response is therefore a layered model combining strong authentication, email and endpoint protection, contextual training, supportive reporting mechanisms and rapid incident response. The principal lesson for post-pandemic cybersecurity is that remote-work resilience depends not on eliminating human error but on designing systems capable of preventing a single deceptive interaction from becoming a major organisational compromise.

## Declarations

### Author Contributions

Conceptualization, review design, literature synthesis, analysis, writing - original draft, and writing - review and editing.


### Funding

This research received no external funding.


### Ethics Statement

Not applicable. This review article synthesised previously published literature and did not involve primary research with human participants or animals.

### Informed Consent

Not applicable.

### Data Availability

No new datasets were generated or analysed for this review. The evidence base is represented by the published sources cited in the article.

### Conflicts of Interest

The author declares no conflict of interest.

## References


Aleroud, A. and Zhou, L. (2017) 'Phishing environments, techniques, and countermeasures: A survey', Computers & Security, 68, pp. 160–196.

Alshaikh, M. (2020) 'Developing cybersecurity culture to influence employee behavior: A practice perspective', Computers & Security, 98, 102003.

Bauer, S., Bernroider, E.W.N. and Chudzikowski, K. (2017) 'Prevention is better than cure! Designing information security awareness programs to overcome users' non-compliance with information security policies in banks', Computers & Security, 68, pp. 145–159.

Chen, R., Gaia, J. and Rao, H.R. (2020) 'An examination of the effect of recent phishing encounters on phishing susceptibility', Decision Support Systems, 133, 113287.

Chowdhury, N.H., Adam, M.T.P. and Teubner, T. (2020) 'Time pressure in human cybersecurity behavior: Theoretical framework and countermeasures', Computers & Security, 97, 101963.

Da Veiga, A., Astakhova, L.V., Botha, A. and Herselman, M. (2020) 'Defining organisational information security culture—Perspectives from academia and industry', Computers & Security, 92, 101713.

De, R., Pandey, N. and Pal, A. (2020) 'Impact of digital surge during COVID-19 pandemic: A viewpoint on research and practice', International Journal of Information Management, 55, 102171.

Frauenstein, E.D. and Flowerday, S. (2020) 'Susceptibility to phishing on social network sites: A personality information processing model', Computers & Security, 94, 101862.

Goel, D. and Jain, A.K. (2018) 'Mobile phishing attacks and defence mechanisms: State of art and open research challenges', Computers & Security, 73, pp. 519–544.

Gratian, M., Bandi, S., Cukier, M., Dykstra, J. and Ginther, A. (2018) 'Correlating human traits and cyber security behavior intentions', Computers & Security, 73, pp. 345–358.

Han, J.Y., Kim, Y.J. and Kim, H. (2017) 'An integrative model of information security policy compliance with psychological contract: Examining a bilateral perspective', Computers & Security, 66, pp. 52–65.

Hooper, V. and Blunt, C. (2020) 'Factors influencing the information security behaviour of IT employees', Behaviour & Information Technology, 39(8), pp. 862–874.

House, D. and Raja, M. (2020) 'Phishing: Message appraisal and the exploration of fear and self-confidence', Behaviour & Information Technology, 39(11), pp. 1204–1224.

Karjalainen, M., Siponen, M. and Sarker, S. (2020) 'Toward a stage theory of the development of employees' information security behavior', Computers & Security, 93, 101782.

Ki-Aries, D. and Faily, S. (2017) 'Persona-centred information security awareness', Computers & Security, 70, pp. 663–674.

Li, L., He, W., Xu, L., Ash, I., Anwar, M. and Yuan, X. (2019) 'Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behavior', International Journal of Information Management, 45, pp. 13–24.

Li, Y., Zhang, N. and Siponen, M. (2019) 'Keeping secure to the end: A long-term perspective to understand employees' consequence-delayed information security violation', Behaviour & Information Technology, 38(5), pp. 435–453.

Menard, P., Warkentin, M. and Lowry, P.B. (2018) 'The impact of collectivism and psychological ownership on protection motivation: A cross-cultural examination', Computers & Security, 75, pp. 147–166.

Mouton, F., Leenen, L. and Venter, H.S. (2016) 'Social engineering attack examples, templates and scenarios', Computers & Security, 59, pp. 186–209.

Öğütçü, G., Testik, Ö.M. and Chouseinoglou, O. (2016) 'Analysis of personal information security behavior and awareness', Computers & Security, 56, pp. 83–93.

Papagiannidis, S., Harris, J. and Morton, D. (2020) 'WHO led the digital transformation of your company? A reflection of IT related challenges during the pandemic', International Journal of Information Management, 55, 102166.

Parsons, K., Calic, D., Pattinson, M., Butavicius, M., McCormac, A. and Zwaans, T. (2017) 'The Human Aspects of Information Security Questionnaire (HAIS-Q): Two further validation studies', Computers & Security, 66, pp. 40–51.

Parsons, K., Butavicius, M., Delfabbro, P. and Lillie, M. (2019) 'Predicting susceptibility to social influence in phishing emails', International Journal of Human-Computer Studies, 128, pp. 17–26.

Rajab, M. and Eydgahi, A. (2019) 'Evaluating the explanatory power of theoretical frameworks on intention to comply with information security policies in higher education', Computers & Security, 80, pp. 211–223.

Safa, N.S., Von Solms, R. and Furnell, S. (2016) 'Information security policy compliance model in organizations', Computers & Security, 56, pp. 70–82.

Wiley, A., McCormac, A. and Calic, D. (2020) 'More than the individual: Examining the relationship between culture and Information Security Awareness', Computers & Security, 88, 101640.

## Table 1. Major phishing and credential-security risks for remote employees and corresponding organisational controls

| Risk factor | Remote-working manifestation | Potential attack mechanism | Security consequence | Evidence from literature | Recommended organisational control |
|---|---|---|---|---|---|
| Time pressure and distraction | Employees process email while attending virtual meetings or handling competing domestic/work tasks | Urgent password-reset, invoice, HR or account-verification message | Reduced scrutiny followed by credential submission | Chowdhury, Adam and Teubner (2020); Parsons et al. (2019) | Contextual warnings, delayed high-risk actions, simple reporting mechanisms and phishing simulations |
| Reliance on electronic communication | Instructions previously verified in person arrive through email or collaboration platforms | Executive impersonation, fake IT support or spoofed colleague request | Disclosure of passwords, MFA codes or confidential information | Mouton, Leenen and Venter (2016); Aleroud and Zhou (2017) | Out-of-band verification for sensitive requests and authenticated internal communication |
| Cloud-service dependence | Frequent Microsoft 365, webmail, VPN and SaaS authentication | Replica login pages and credential-harvesting portals | Account takeover and subsequent access to organisational resources | Aleroud and Zhou (2017); Goel and Jain (2018) | Multi-factor authentication, conditional access and centralised identity management |
| Mobile-device usage | Employees inspect messages on smartphones with reduced interface information | Shortened URLs, disguised domains and mobile-optimised phishing pages | Increased difficulty evaluating destination authenticity | Goel and Jain (2018) | Mobile-aware email filtering, managed devices and safer link handling |
| Weak security awareness | Employees know organisational tasks but lack practical threat-recognition skills | Social-engineering cues exploit trust, urgency or authority | Click-through and credential compromise | Parsons et al. (2017); Li et al. (2019) | Role-specific and scenario-based awareness programmes |
| Policy-practice gap | Security procedures are difficult to follow outside the office | Employees bypass inconvenient authentication or reporting procedures | Unsafe workarounds and policy non-compliance | Safa, Von Solms and Furnell (2016); Rajab and Eydgahi (2019) | Simplify secure processes and integrate controls into normal workflows |
| Weak security culture | Remote workers receive fewer informal security reminders and less peer reinforcement | Suspicious events remain unreported or are reported slowly | Extended attacker dwell time and repeated targeting | Da Veiga et al. (2020); Alshaikh (2020) | Supportive reporting culture, management engagement and security champions |
| Overconfidence following training | Employees assume previous training or exposure makes them resistant | Sophisticated or personalised phishing bypasses habitual checks | Misclassification of malicious messages | Chen, Gaia and Rao (2020) | Continuous adaptive training and measurement of behaviour rather than training completion |

*Note. MFA = multi-factor authentication; VPN = virtual private network; SaaS = software as a service.*

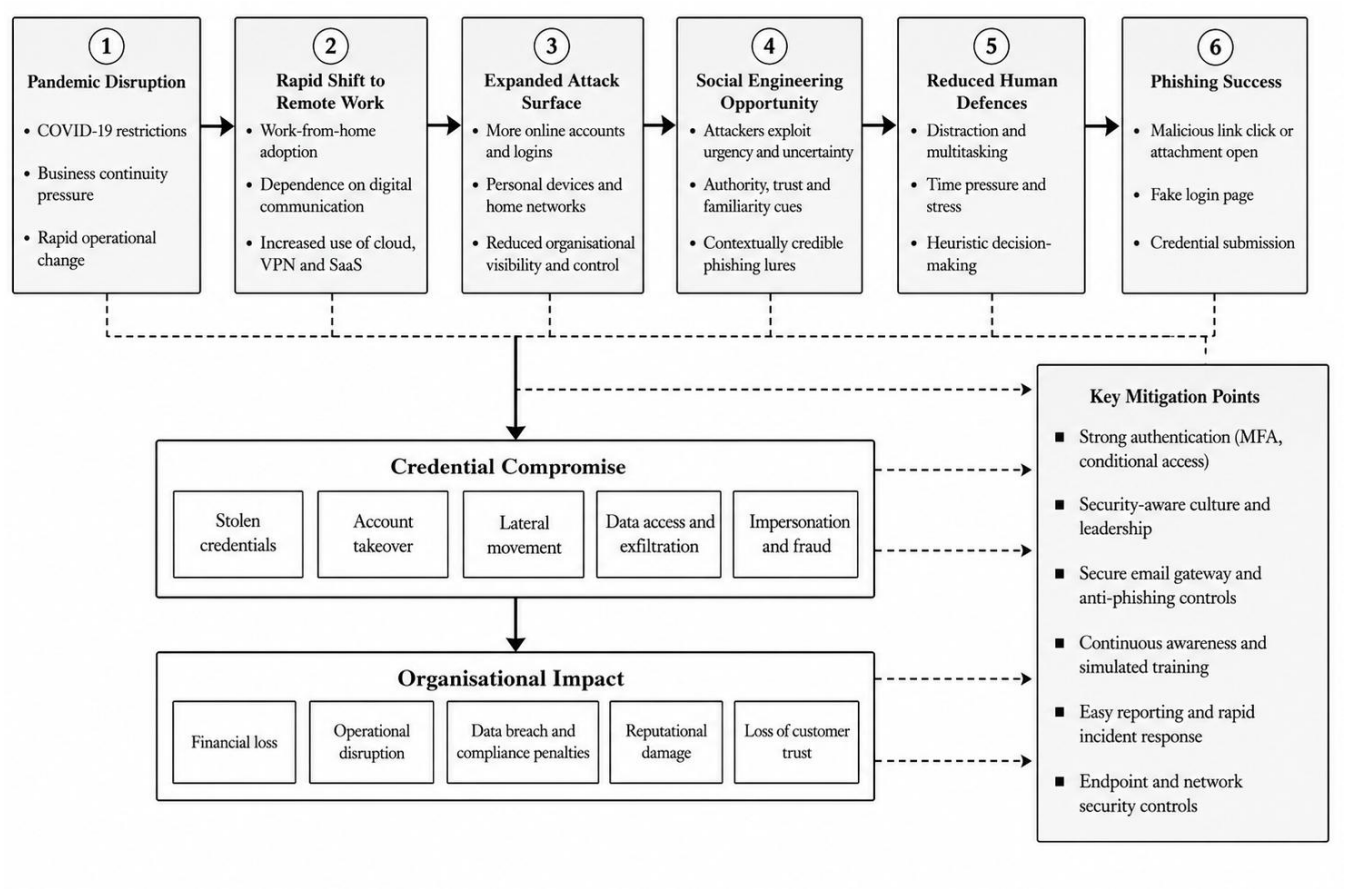


**Figure 1. Pathway from COVID-19 Remote Working to Credential Compromise.**

*Pandemic disruption acts primarily as a threat multiplier. It modifies technological routines and employee decision contexts, thereby increasing opportunities for existing phishing mechanisms.*

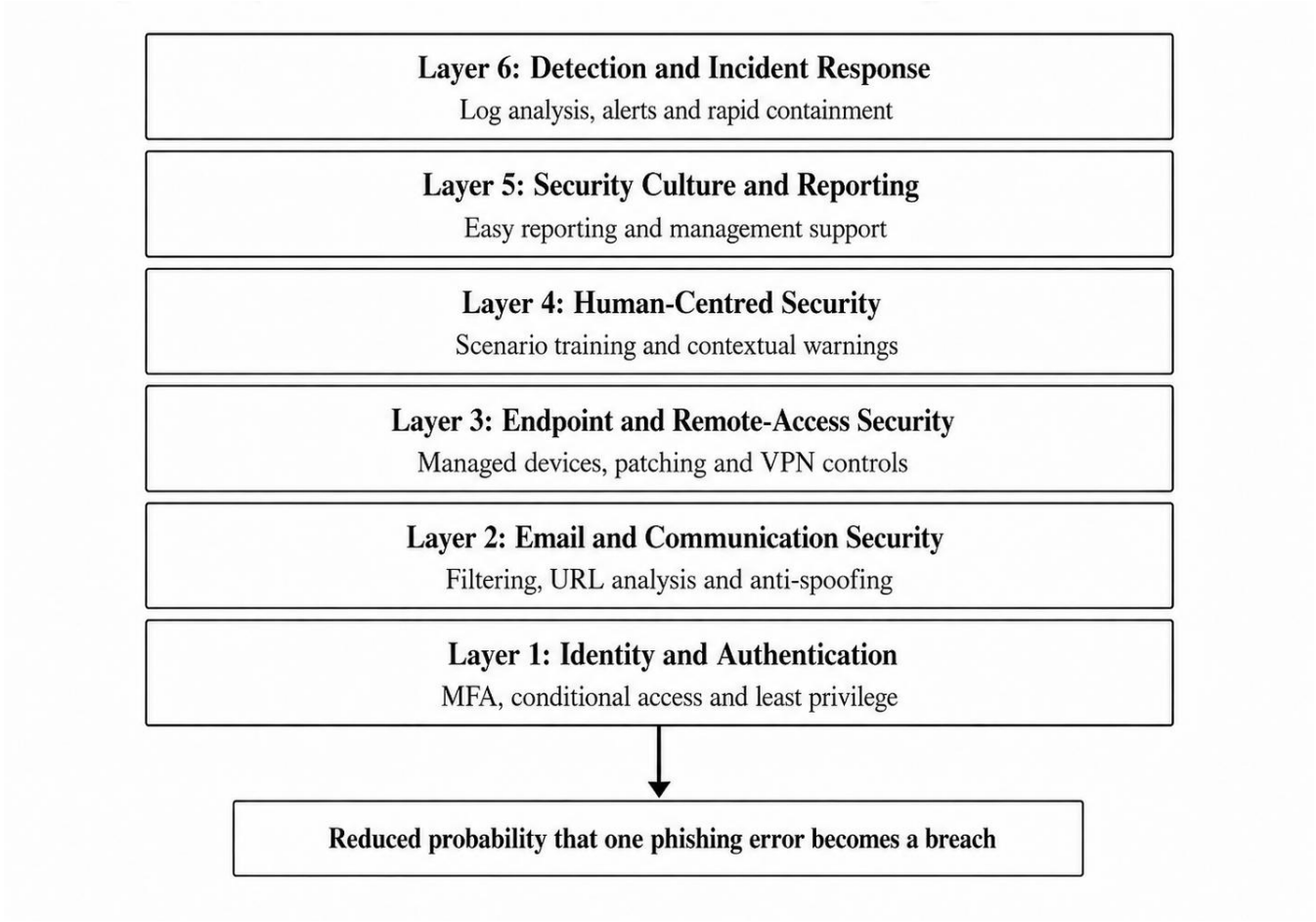


**Figure 2. Layered Defence Model for Remote-Worker Phishing and Credential Threats.**

*Protection should be constructed so that the compromise of a single layer - particularly human recognition - does not provide unrestricted organisational access.*

**How to cite:** Irshad, A. (2021). Phishing and Credential-Based Cybersecurity Threats Among Remote Employees During the COVID-19 Pandemic in the United Kingdom. Journal of Multidisciplinary Research and Integrated Sciences, 1(1), 1-7.