GBS
GLOBAL BANKING SCHOOL

BSU
BATH SPA UNIVERSITY

Module Code	CPUF 100-20C
Module Name	Digital Foundations
Module Leader	Sahiba Akhtar
Cohort	October 2026
Assessment component(s)	Report
Restrictions on time/word count	1500 words
Individual/group	Individual
Assessment weighting(s)	100%
Hand in date(s)	09/02/2026
Student ID	G1485068
Campus	BSUEAST
Module Tutor	
Word Count	1608

Table of Contents

List of Figures

1.0 Introduction

The Digital Foundation module is essential for my success at university alongside building competency in computing settings. The module focused on digital communication, logical thinking and problem solving, and the fundamentals of digital citizenship. This is significant as communication supports teamwork across departments, problem solving reinforces debugging and troubleshooting, and digital citizenship develops awareness of footprints, privacy, and the ethical use of technology and intellectual property.

This report focuses on a cybersecurity breach at Fly-Tech in April 2025. A phishing email targeted staff and several employees fell victim, leading to compromised accounts, password changes, and account lockouts. The situation then escalated because internal communication became fragmented: different platforms were used at once, updates were inconsistent, and the incident was prematurely described as resolved. This increased confusion internally and resulted in reputational damage from stakeholders and clients.

Effective digital communication is crucial during a crisis, especially for a technology-driven organisation like Fly-Tech, because it reduces panic, keeps everyone aligned with information, and helps prevent repeated mistakes. This report will critically evaluate the communication tools used, explain how ethics and digital citizenship link to the incident, and conclude with evidence-based recommendations to effectively prevent and manage similar occurrences in the future.

2.1 Digital Communication Tools Used in the Incident

Figure 1: Logos of three direct messaging apps for business (Skype, Slack and Microsoft Teams) (Derudder, 2020).

2.1.1 Description of the Tools Used

Several digital communication tools were used during the April 2025 cybersecurity incident at Fly-Tech. Email (Microsoft 365/Outlook) was used for internal and client communication, and it was also the method used to deliver the phishing email that triggered the breach (Appendix A). Microsoft Teams was Fly-Tech's main internal collaboration tool and was used for staff messaging, including early informal reports of login issues (Appendix B).

WhatsApp was utilised in an unofficial manner, as a quick messaging platform for sharing updates between staff (Appendix C). Zoom was used as the video-conferencing tool for a meeting intended to coordinate next steps during the incident (Appendix D). Finally, social media was used for external communication, specifically X/Twitter, where Fly-Tech posted public updates about service status (Appendix E). Following this, stakeholders and clients also raised concerns through external email and social media channels (Appendix F).

2.1.2 Evaluation of Appropriate Use

Email was the most formal and professional channel for official updates; however, it was also the method used to deliver the phishing message (Appendix A). Accessibility was impacted because account lockouts meant some staff could not receive guidance, and while email is normally traceable through audit trails, compromised accounts reduce confidence in message authenticity. Evidence also suggests that phishing training does not fully remove user susceptibility, meaning email remains a high-risk channel in practice (Marshall, Sturman and Auton, 2024). Overall, email was only partly effective during the crisis.

Microsoft Teams supported fast internal communication; but, in this incident, it remained informal and lacked a clear, centralised announcement space (Appendix B). Accessibility was generally good for staff with Teams access, and traceability is strong because Teams content can be preserved and retrieved through eDiscovery and audit capabilities (Microsoft, 2025a). Overall, Teams was moderately effective but needed stronger structure and ownership.

WhatsApp enabled rapid messaging, but it was informal and not inclusive because not all departments were added (Appendix C). It also creates governance issues, as official information in non-corporate channels can be difficult to manage and retrieve appropriately (ICO, n.d.). Overall, WhatsApp was ineffective as a primary crisis tool.

Zoom was appropriate for real-time coordination, but accessibility was reduced because the meeting was announced only via WhatsApp (Appendix D). Security depends on consistent use of controls such as locks and waiting rooms (Zoom Video Communications, Inc., n.d.). Overall, Zoom could have been effective, but poor distribution limited its value.

X/Twitter was fast for stakeholder updates, but the premature "restored" message shows the reputational risk of unverified public communication (Appendix E). Trust can quickly degrade during crises when social media communication is mishandled (Shahbazi and Bunker, 2024). Overall, X/Twitter was ineffective in this incident.

2.1.3 Identification of Failure Points

Communication failure begins externally when a credible phishing email is delivered successfully and engaged with by multiple staff (Appendix A). The first internal failure occurs when login issues are reported informally on Teams without a central alert, owner, or coordinated IT instruction to stop interacting with the message (Appendix B). The situation escalates as staff move to an unofficial WhatsApp group not joined by all departments, creating uneven awareness and fragmented decision-making (Appendix C). This widens when the Zoom meeting is announced only via WhatsApp, excluding unincluded staff (Appendix D). The most damaging escalation is the unverified "restored" tweet (Appendix E).

2.1.4 Analysis of Root Issues

These failures occurred because both external and internal communication controls were weak. Externally, the phishing email reaching multiple inboxes suggests gaps in inbound filtering and link/attachment protection, meaning a malicious message could enter the organisation and then trigger avoidable account compromises (Appendix A). Internally, there was no established incident communication plan or clear ownership for issuing authoritative updates, so early Teams reports did not convert into an organisation-wide warning or single source of truth (Appendix B). This increased impact because staff defaulted to the fastest tools, creating parallel conversations across Teams and WhatsApp and causing departments to act on different information (Appendices B–D). Account lockouts then reduced access to core channels, increasing reliance on personal devices and informal messaging, which reduced oversight and consistency (Appendices C–D). The premature "restored" tweet suggests external messaging was not tied to internal technical confirmation, undermining trust and driving complaints when issues persisted (Appendices E–F).

2.1.5 Overall Evaluation

Overall, Fly-Tech managed the incident reactively rather than systematically. A strength was that staff identified and shared early symptoms quickly through peer reporting (Appendix B). However, the organisation did not control communication flow: the initial phishing message was able to spread into the business (Appendix A), and once disruption began there was no single internal channel or verified instruction set, resulting in fragmented coordination across Teams, WhatsApp and Zoom (Appendices B–D). External communication was also poorly governed, shown by the unverified "restored" tweet, which amplified confusion and reputational impact through stakeholder complaints (Appendices E–F). The delayed start of formal audit and crisis planning indicates slow escalation (Appendix H), reducing confidence and clarity internally (Appendix G).

2.1.6 Recommendations for Future Cyber Crisis Management

Within 45 days, strengthen email and browsing protections to reduce the chance that external communication failures become internal disruption. Implement URL time-of-click protection and attachment sandboxing (e.g., Microsoft Safe Links/Safe Attachments), and ensure suspicious links are blocked before users can access them (Microsoft, 2025b; Microsoft, 2025c).

Within 60 days, Fly-Tech should publish a crisis communication policy that sets a single internal incident channel, assigns an incident communications lead, and requires technical verification before any organisation-wide or public updates are released (NIST, 2025, p. 13).

Within 90 days, introduce mandatory training and exercises covering phishing recognition, secure tool use, and digital ethics, with 100% completion tracked and quarterly refreshers (NIST, 2024, pp. 4–5). To rebuild trust, adopt timed stakeholder updates via a controlled status page and only declare "restored" once internally confirmed (NCSC, 2024).

Figure 2: NIST Cybersecurity Framework functions (Identify, Protect, Detect, Respond, Recover) (NIST, 2018).

3.0 Ethics and Digital Citizenship

The incident raised ethical concerns around privacy, confidentiality, and Fly-Tech's duty of care as a technology provider to education clients. As compromised Fly-Tech accounts sent suspicious emails to clients (Appendix F), personal data may have been affected through unauthorised disclosure, alteration, or loss of availability. UK GDPR defines a personal data breach as a security breach affecting the confidentiality, integrity, or availability of personal data (European Union, 2016). Even if the scale was unclear initially, ethical practice requires early assessment, evidence preservation, and accountable decision-making to reduce harm and protect individuals (ICO, 2025).

Additionally, Fly-Tech holds responsibility for preventing predictable risks, not only reacting to staff error. The incident began as an external communication failure: a phishing email entered the organisation and prompted credential submission (Appendix A), which then created internal disruption through account compromise and lockouts. Ethically, Fly-Tech should reduce avoidable exposure through layered controls on inbound email and web access, rather than relying on perfect user judgement. Industry evidence supports this approach, as the Verizon DBIR highlights social engineering and credential theft as persistent contributors to breaches (Verizon, 2024).

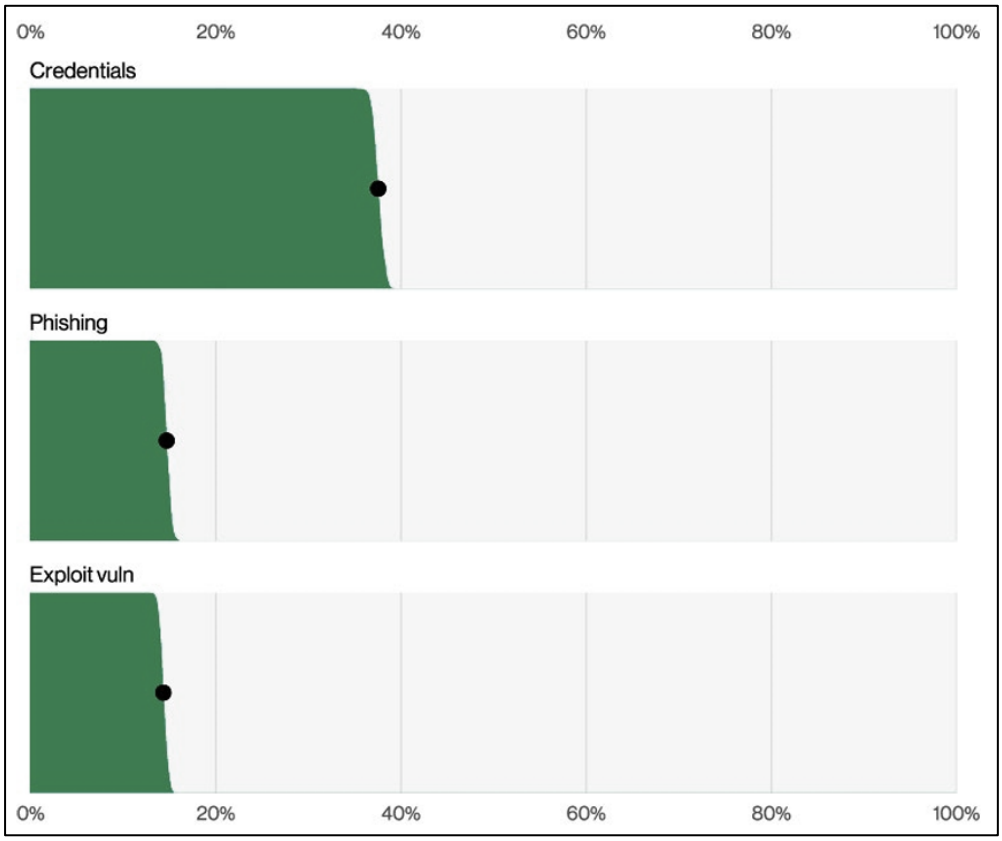

Figure 3: Common initial access methods in non-error, non-misuse data breaches (n = 6,963) (Verizon, 2024).

Communication ethics were also weak. Publishing an unverified “restored” tweet (Appendix E) prioritised reassurance over accuracy, likely lowering stakeholder vigilance and damaging trust when issues persisted (Appendix F). ENISA guidance stresses using a communication plan with defined roles and agreed stakeholder messaging to maintain transparency without misinformation (ENISA, 2025). Improving digital citizenship therefore requires staff to follow reporting routes, protect confidentiality, avoid informal incident coordination spaces, and recognise that digital footprints can have lasting reputational impact.

4.0 Conclusion

The Fly-Tech incident demonstrates that cyber crises are as much communication failures as technical events. Fragmented channels, unclear ownership, and unverified external messaging weakened organisational control, allowing a contained phishing attack to escalate into operational and reputational harm. The breach revealed a structural misalignment between communication governance, ethical responsibility, and security practice, showing that resilience depends on disciplined information management as well as technical safeguards.

Future preparedness requires an integrated communication framework where authority, verification, and channel governance are predefined. A single source of truth, formal escalation triggers, and verified public messaging would reduce ambiguity, while embedding digital citizenship through training strengthens accountability. Aligning technical controls with strategic communication governance is therefore essential for protecting trust and sustaining operational credibility.

References

ENISA (2025) ENISA Technical Implementation Guidance (version 1.0). Available at: https://www.enisa.europa.eu/sites/default/files/2025-06/ENISA_Technical_implementation_guidance_on_cybersecurity_risk_management_measures_version_1.0.pdf (Accessed: 7th January 2026).

European Union (2016) Regulation (EU) 2016/679 (General Data Protection Regulation), Article 32 and Article 4 (Definitions). Available at: https://www.legislation.gov.uk/eur/2016/679/article/4 (Accessed: 7th January 2026).

Information Commissioner's Office (ICO) (2025) Personal data breaches: a guide. Available at: https://ico.org.uk/for-organisations/report-a-breach/personal-data-breach/personal-data-breaches-a-guide/ (Accessed: 7th January 2026).

Information Commissioner's Office (ICO) (n.d.) Official information held in non-corporate communications channels. Available at: https://ico.org.uk/for-organisations/foi/freedom-of-information-and-environmental-information-regulations/official-information-held-in-non-corporate-communications-channels/ (Accessed: 6th January 2026).

Marshall, N., Sturman, D. and Auton, J.C. (2024) 'Exploring the evidence for email phishing training: A scoping review', Computers & Security, 139, 103695. Available at: https://doi.org/10.1016/j.cose.2023.103695 (Accessed: 5th January 2026).

Microsoft (2025a) Finding content in Microsoft Teams in eDiscovery. Available at: https://learn.microsoft.com/en-us/purview/edisc-search-teams (Accessed: 6th January 2026).

Microsoft (2025b) Safe Links in Microsoft Defender for Office 365. Available at: https://learn.microsoft.com/en-us/defender-office-365/safe-links-about (Accessed: 7th January 2026).

Microsoft (2025c) Safe Attachments in Microsoft Defender for Office 365 (overview). Available at: https://learn.microsoft.com/en-us/defender-office-365/safe-attachments-about (Accessed: 7th January 2026).

National Cyber Security Centre (NCSC) (2024) Guidance on effective communications in a cyber incident. Available at: https://www.ncsc.gov.uk/guidance/effective-communications-in-a-cyber-incident (Accessed: 6th January 2026).

National Institute of Standards and Technology (NIST) (2024) Building a Cybersecurity and Privacy Learning Program (Special Publication 800-50 Revision 1). Available at: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-50r1.pdf (Accessed: 6th January 2026).

National Institute of Standards and Technology (NIST) (2025) Incident Response Recommendations and Considerations for Cybersecurity Risk Management (NIST Special Publication 800-61 Revision 3). Available at: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r3.pdf (Accessed: 6th January 2026).

Shahbazi, M. and Bunker, D. (2024) 'Social media trust: Fighting misinformation in the time of crisis', International Journal of Information Management, 77, 102780. Available at: https://doi.org/10.1016/j.ijinfomgt.2024.102780 (Accessed: 6th January 2026).

Verizon (2024) 2024 Data Breach Investigations Report (DBIR). Available at: https://www.verizon.com/business/resources/reports/2024-dbir-data-breach-investigations-report.pdf (Accessed: 7th January 2026).

Zoom Video Communications, Inc. (n.d.) Best Practices for Securing Your Zoom Meetings. Available at: https://explore.zoom.us/docs/doc/Securing%20Your%20Zoom%20Meetings.pdf (Accessed: 6th January 2026).