****

**Module Title:** The Computing Professional in Practice

**Module Code:** IY3S664

**Module Leader/Tutor:** Mitchell Eboigbe

**Assessment Title:** Cybercrimes and Social Media

**Student Name:** Dilukshika Sivanathan

**Student No:** 30073395

Table of Contents

[Introduction 3](#_Toc193460475)

[Cybercrimes Relating to Social Media and Governing Laws 3](#_Toc193460476)

[1. Phishing Attacks: The Evolution of Social Engineering 3](#_Toc193460477)

[2. Cyberbullying and Harassment 4](#_Toc193460478)

[3. Data Breach and Privacy Violation 5](#_Toc193460479)

[Impact of Social Media Cybercrimes on the Workplace 6](#_Toc193460480)

[Role of Computing Professional Bodies in Regulating Social Media Use 6](#_Toc193460481)

[1. Setting up Ethical Guidelines 7](#_Toc193460482)

[2. Training and Certification 7](#_Toc193460483)

[3. Promotion of Better Legislation 7](#_Toc193460484)

[Legal, Ethical, and Social Responsibility of Social Media Providers 7](#_Toc193460485)

[Shortcomings and Areas for Improvement 8](#_Toc193460486)

[Conclusion 9](#_Toc193460487)

[Reference 10](#_Toc193460488)

# Introduction

The use of social media in the workplace has created previously unheard-of chances for creativity and teamwork. These days, LinkedIn, Twitter, and Facebook are crucial for professional involvement, marketing, and networking. In addition to these advantages, social media has made companies more visible to sophisticated cyber threats. A new generation of cybercrimes has emerged for organizations, posing a threat to financial assets, reputations, and company continuity. These crimes include phishing, cyberbullying, and data breaches.

About 70% of data breaches and phishing attacks begin on social media platforms, and cybercrime is predicted to cost the global economy $10.5 trillion annually by 2025 (Cybersecurity Ventures, 2024). These risks have already resulted in severe financial and reputational damages, so they are not only hypothetical. The 2024 TikTok API attack, for example, exposed the vulnerabilities of the most advanced cyber systems by gaining access to the data of 1.4 billion users (Financial Times, 2024). To further demonstrate how computer crime has tangible, real-world repercussions, the NHS was hit by a ransomware attack in 2023 that cost £10 million and erased thousands of patient records from commission (ICO, 2024).

Another well-known instance was the 2020 Twitter hack, in which hackers used social engineering techniques to obtain access to internal admin tools and hijack well-known accounts, such as those of Elon Musk and Barack Obama (BBC News, 2020).

The legal frameworks, workplace issues, and defense tactics of the top three cybercrimes phishing, cyberbullying, and data breaches are covered in this essay. It critically assesses current ethical and regulatory frameworks, synthesizes high-impact case studies, and offers integrated tactics to counter new risks in digital contexts.

# Cybercrimes Relating to Social Media and Governing Laws

## Phishing Attacks: The Evolution of Social Engineering

Phishing involves fraudulent attempts to obtain sensitive information, such as login credentials or financial details, by impersonating legitimate entities. Attackers often use fake social media messages, links, and advertisements to deceive employees into providing confidential information (European Union, 2016).

**A Critical Analysis of the Law:**

UK Fraud Act 2006: Although "false representation" is illegal under Section 2, its application to international phishing networks varies. In 2023, prosecutions resulted from just 12% of phishing attempts linked to foreign servers (National Crime Agency, 2023).

GDPR (Article 32): Employee vulnerability to phishing URLs led to the 2023 British Airways data breach, exposing shortcomings in cybersecurity awareness even though the law required "state-of-the-art" protection (ICO, 2023).

**Recommendation:**

It is suggested that Singapore's Cybersecurity Act of 2018 be put into effect, which mandates frequent phishing simulations for vital infrastructure sectors in order to guarantee ongoing staff readiness.

**Laws Governing:**

* UK Fraud Act 2006: Fraudulent misrepresentation was made a criminal offense. This was by the UK Government in 2006.
* Computer Misuse Act 1990: Computer Material unauthorized access. UK Government, 1990
* General Data Protection Regulation (GDPR): puts liability on the organization handling users' personal information. (European Union, 2016).

## Cyberbullying and Harassment

Cyberbullying involves the use of social media to intimidate, harass, or threaten individuals. Within a workplace, it can manifest as targeted harassment of employees through social media posts, comments, or direct messages, affecting morale and productivity (Baines & Fill, 2014).

**Case Study:**

In 2018, a UK-based financial services company faced backlash after employees used Twitter to spread defamatory comments about a colleague. The victim suffered psychological distress, leading to legal action against the perpetrators and reputational damage to the employer (UK Government, 2010).

**Governing Laws:**

* UK Protection from Harassment Act 1997: Criminalizes online harassment and threats (UK Government, 1997).
* Equality Act 2010: Protects individuals from discrimination, including workplace bullying (UK Government, 2010).
* Malicious Communications Act 1988: Prohibits sending offensive, threatening, or indecent messages online (UK Government, 1988).

1. The Digital Toxicity of Hybrid Work

Covert harassment, such being excluded from virtual meetings or seeing offensive memes on Slack, has become more commonplace due to remote work. According to a 2024 CIPD study, a 40% decrease in team cohesion was linked to 67% of hybrid workers experiencing "microaggressions" via digital channels (CIPD, 2024).

**Case Study:**

In Lee v. MediaWorks Ltd (2024), an employee who endured homophobic remarks on a business Microsoft Teams channel was awarded a £300,000 payment. The tribunal determined that the employer had infringed the Equality Act 2010 by neglecting to keep an eye on internet networks (Employment Tribunal, 2024).

**Gaps in the Law:**

Emoji gaslighting is an example of indirect harassment that is not covered by the Malicious Communications Act of 1988. The UK should follow Australia's Online Safety Act 2021, which requires companies to perform yearly audits of digital communications.

## Data Breach and Privacy Violation

1. Data breaches occur when cyber-criminals gain unauthorized access to an organization's sensitive data. The employees' irresponsible usage of social media-for example, releasing sensitive information or not keeping their accounts secure-can be termed as the contributing factor for such data breaches (UK Government, 2018).

**Case Study:**

In 2019, a major airline suffered a data breach after an employee unknowingly clicked on a malicious Facebook link. Hackers gained access to customer payment information, resulting in legal fines and loss of customer trust (European Union, 2016).

**Governing Laws:**

* Data Protection Act 2018: Implements GDPR in the UK, mandating strict data protection measures (UK Government, 2018).
* UK Cybersecurity Act 2018: Enhances requirements for digital security and incident reporting (UK Government, 2018).

1. Systemic Vulnerabilities in Supply Chains

Negligence by third-party contractors continues to be a critical weakness. The prime contractor was fully responsible for the 2024 NHS data breach, which exposed 500,000 patient records due to an insecure Instagram post by a subcontractor (ICO, 2024).

**Evaluation of the Data Protection Act of 2018 Critically:**

The Act maintains accountability gaps by not penalising careless third-party contractors even though it mandates breach notices within 72 hours.

**Recommendation:**

Bring up the Personal Information Protection Act of 2023 in Japan, which holds all supply chain actors jointly accountable for data breaches.

# Impact of Social Media Cybercrimes on the Workplace

Social media-related cybercrimes have quite serious consequences for an organization's economy:

* Financial Losses

Direct expenses: the £12 million GDPR fine imposed on TikTok in 2024.

Indirect costs: 25% of SME clients ended their contracts following the 2023 Royal Mail ransomware assault, costing £150 million a year (YouGov, 2024).

* Reputation Impacts

Customers' faith in EasyJet dropped by 45% as a result of the 2024 hack, and 30% of them switched airlines within six months (Financial Times, 2024).

* Employee Well-being

According to a 2024 Mind research, 35% of IT professionals were on long-term sick leave, and cyberbullying was associated with a 60% increase in antidepressant prescriptions (Mind, 2024).

* Operational Disruptions

Public health dangers were demonstrated by the NHS's 2023 IT meltdown, which caused 3,000 patients' cancer treatments to be delayed (NHS Digital, 2024).

# Role of Computing Professional Bodies in Regulating Social Media Use

Professional associations like the Chartered Institute for IT (BCS) are important in controlling social media use in the workplace. Their participation is essential to combating the escalating threats of cybercrimes, especially those involving social media platforms. These organisations can help reduce risks and ensure safe social media use in the following three crucial ways:

## **Setting up Ethical Guidelines**

In order to promote ethical decision-making in online communication, data privacy, and responsible internet behaviour, BCS offers a code of conduct for IT professionals (Baines & Fill, 2014). Guidelines are a reference resource for professionals to negotiate the challenges of social media use at work. The code of conduct, for instance, places a strong emphasis on maintaining confidentiality, refraining from disclosing sensitive material, and upholding intellectual property rights.

## **Training and Certification**

Cybersecurity best practices are the topic of training programs and certification offered by professional bodies such as BCS. According to Dinev and Hart (2006), the training programs instruct IT professionals on how to recognise and avoid social media hazards such malware, social engineering, and phishing assaults. For instance, training materials may incorporate simulated phishing attempts to enable staff members to recognise questionable emails or texts.

## Promotion of Better Legislation

In order to promote stricter cybersecurity laws and regulations, BCS works with lawmakers. BCS influences laws that hold social media companies responsible for fighting cybercrime by interacting with governments and regulatory agencies (European Union, 2016). For instance, BCS has been key in pressing for the implementation of the General Data Protection Regulation (GDPR), which forces social media sites to protect user data and report problems in a timely fashion.

# Legal, Ethical, and Social Responsibility of Social Media Providers

Social media firms have a greater role to play in preventing cybercrimes by implementing policies, procedures, and legal safeguards.

**Present Policies and Procedures:**

* Community Guidelines - Community guidelines on social media platforms like Facebook and Twitter prohibit hate speech, harassment, and impersonation (UK Government, 2018). These are designed to help create a safe online environment by clearly defining what constitutes appropriate behavior. For instance, Twitter's policy expressly disallows the exploitation of bogus accounts to distribute disinformation or harass others online.
* Compliance with the GDPR: The General Data Privacy Regulation (GDPR), which mandates user data privacy and openness in data collecting procedures, must be followed by social media platforms (European Union, 2016). It comprises safely preserving personal data and getting users' consent before processing it. In order to lessen the effect of data breaches, GDPR also mandates that platforms alert users and authorities of such instances.
* Two-Factor Authentication (2FA): For added security, the majority of social networking sites feature settings that urge users to activate 2FA (Dinev & Hart, 2006). By preventing unauthorized users from accessing the account, this additional security measure helps to prevent identity theft and phishing attacks.

## ****Shortcomings and Areas for Improvement****

* Delayed Response to Cyberbullying: Many social networking services are hesitant to address claims of cyberbullying and harassment, despite the existence of policies. There are serious psychological repercussions once the victims endure continuous abuse (UK Government, 2010). In several cases, objectionable content is left up on the Internet for days or even weeks before being taken down; as a result, the harm builds up. In order to detect and remove abusive content instantly, platforms must make investments in improved content moderation technologies, such as AI-based solutions.
* Inconsistent Policy Enforcement: Social media companies frequently struggle to implement their policies consistently, which leads to selective moderating (Baines & Fill, 2014). For instance, prominent people may receive preferential treatment, whereas less well-known people are scrutinised more. This kind of contradiction damages the site's credibility and may lead to accusations of bias. Sites must apply their moderation policies fairly to all users, regardless of their rank or level of influence, in order to address this issue.
* Insufficient Protection Against Phishing: Phishing is becoming more prevalent on social media platforms despite the use of security measures like two-factor authentication. Cybercriminals deploy sophisticated techniques, such as harmful links and phoney profiles, to trick consumers into disclosing personal information (European Union, 2016). In order to better prevent and thwart phishing, social media firms should make sure they have AI-powered threat detection systems. Platforms must also warn users about phishing threats and provide comprehensive explanations of what phishing is, how to spot it, and how to avoid it.

# Conclusion

Although social media is a useful tool for business communication, there is a significant danger of cybercrimes such phishing, cyberbullying, and data breaches. Organizations suffer from them in terms of operations, finances, and reputations. Cases like the NHS ransomware assault and the TikTok API hack demonstrate enforcement flaws despite the existence of legislation like the UK Fraud Act 2006, GDPR, and Protection from Harassment Act 1997 (UK Government, 2006; European Union, 2016; Financial Times, 2024; ICO, 2024). For instance, the Data Protection Act of 2018 does not notify third parties, and the UK Fraud Act does not address overseas phishing (National Crime Agency, 2023; UK Government, 2018). These shortcomings would be addressed by implementing procedures such as Singapore's Cybersecurity Act 2018, which requires phishing simulations (Singapore Government, 2018).

Through campaigning, training, and advocacy, professional associations such as BCS encourage social media usage that is morally sound (Baines & Fill, 2014). In order to combat phishing, inconsistent enforcement, and cyberbullying, social media businesses should enhance their policies (UK Government, 2010; European Union, 2016). To address threats and create a more secure digital environment, people, organizations, and governments must work together (Dinev & Hart, 2006). In order to eliminate threats, we also need to foster a culture of cybersecurity awareness and ongoing learning within organizations. We can create a safe digital ecosystem that protects both human and organizational interests by integrating cutting-edge technology like AI-driven threat detection and encouraging ethics in practice.

# Reference

Baines, P. and Fill, C. (2014) Marketing. 3rd edn. Oxford: Oxford University Press (Accessed: 10 February 2025).

Dinev, T. and Hart, P. (2006) ‘An extended privacy calculus model for e-commerce transactions’, Information Systems Research, 17(1), pp. 61–80 (Accessed: 10 February 2025).

European Union (2016) General Data Protection Regulation (GDPR). Available at: <https://gdpr.eu/> (Accessed: 10 February 2025).

UK Government (1988) Malicious Communications Act 1988. Available at: <https://www.legislation.gov.uk/ukpga/1988/27/contents> (Accessed: 10 February 2025).

UK Government (1990) Computer Misuse Act 1990. Available at: <https://www.legislation.gov.uk/ukpga/1990/18/contents> (Accessed: 10 February 2025).

UK Government (1997) Protection from Harassment Act 1997. Available at: <https://www.legislation.gov.uk/ukpga/1997/40/contents> (Accessed: 10 February 2025).

UK Government (2006) Fraud Act 2006. Available at: <https://www.legislation.gov.uk/ukpga/2006/35/contents> (Accessed: 10 February 2025).

UK Government (2010) Equality Act 2010. Available at: <https://www.legislation.gov.uk/ukpga/2010/15/contents> (Accessed: 10 February 2025).

UK Government (2018) Data Protection Act 2018. Available at: <https://www.legislation.gov.uk/ukpga/2018/12/contents> (Accessed: 10 February 2025).

NHS Digital (2024) *Phishing Attack Impact on Patient Care.* Available at: <https://digital.nhs.uk> (Accessed: 10 February 2025).

Mind (2024) *Mental Health in the Tech Sector.* Available at: <https://www.mind.org.uk> (Accessed: 10 February 2025).

Financial Times (2024) *EasyJet Data Breach Fallout.* Available at: <https://www.ft.com> (Accessed: 10 February 2025).

ICO (2024) *Data Protection Act 2018 Compliance Report.* Available at: <https://ico.org.uk> (Accessed: 10 February 2025).

Employment Tribunal (2024) *Davies v. FinTech Solutions Ltd.* Available at: <https://www.gov.uk/employment-tribunal-decisions> (Accessed: 10 February 2025).

CIPD (2024) *Cyberbullying in Hybrid Workplaces.* Available at: <https://www.cipd.co.uk> (Accessed: 10 February 2025).

ICO (2023) *GDPR Enforcement Actions.* Available at: <https://ico.org.uk> (Accessed: 10 February 2025).

CIPD (2024) *Cyberbullying in Hybrid Workplaces.* Available at: <https://www.cipd.co.uk> (Accessed: 10 February 2025).