**Social Media and Business: Profits and Pitfalls**

*Executive Summary*

Focusing on the use of social media for business, this paper begins by exploring how companies can best harness the opportunities offered by platforms such as LinkedIn, Facebook, Twitter and YouTube. Well-crafted content can enhance a commercial footprint and improve search engine rankings, attracting new customers and encouraging brand loyalty. Yet the use of social media also raises questions about the responsibilities of companies to keep customers informed about problems. While clients now expect early disclosure in the public domain, passing on bad news can impact business confidence.

The paper continues with a brief discussion of privacy, noting that many people do not appreciate that the posts they make on social media are essentially open to public view: even if they have implemented privacy settings, there are no guarantees that the information they post will remain private. For businesses, difficulties can also arise when a member of staff shares company information on their private accounts inappropriately or criticises their employer openly.

The next section of the paper comprises an overview of phishing scams, detailing the methods used by both cybercriminal gangs and state-sponsored APTs to dupe individuals and employees into inadvertently providing them with the information they need to hack into a company’s network, or to carry out a successful Business Email Compromise (BEC) campaign. Following on from this, suggestions are given about relevant cybersecurity training for all staff in all organisations – from the post room to the boardroom.

We conclude that it is essential for companies to develop a specific social media policy for all employees, with clear guidance on the posting of both personal and corporate information. A small team of employees should also be given responsibility for the operation of corporate accounts.

*Keywords*: social media, phishing, BEC, COVID-19, cybercrime, cybersecurity, 2FA, Twitter, Facebook, LinkedIn, Instagram, YouTube

*Using social media*

Social media’s growth in the last decade has fundamentally changed the way in which we live our lives: from our interactions with friends and families, the way we pick up the news, how we are influenced by advertising, the way we identify the companies that we trust, and even who we vote for. Twitter, Facebook, Instagram, LinkedIn and YouTube - to name just a few - are among the most widely used social media platforms, but online forums covering both individual and professional interests are also popular.

While social media plays an important part in the lives of hundreds of millions of individuals, companies are also aware that it can be leveraged to their advantage. Its careful use can increase a commercial footprint and improve search engine rankings, thereby attracting new customers and enhancing brand loyalty. It is also extremely cost-effective in marketing terms, as is easily demonstrated. You only have to run a search on Google for adverts to start appearing on your Facebook page or on the sidebars of other websites which you might be visiting.

One survey carried out in 2019 found the following:

* *77% of consumers are more likely to buy from businesses/brands they follow on Social Media.*
* *54% of Social browsers are using Social Media to research products.*
* *71% of consumers who had a positive experience with a business on Social Media are likely to recommend the business to their friends.*
* *Non-Customers are 3 times more likely than customers to visit retailers from Social Media ads.[[1]](#endnote-1)*

Social media networks now form a major role in marketing strategy for all types of company, from small businesses to multinational corporations. As well as offering easy ways of communicating with customers, they are extremely cost-effective.

By using these platforms to promote services or launch new products, companies are also encouraging customer feedback, serving as a kind of market research into how a new product is being received. They can also be used to report problems: product recall, for example, can be communicated much more easily on social media, and will reach exponentially more people when posts are shared than could have been traditionally via email or telephone.

Complaints and compliments can both be acknowledged and easily dealt with: customers can take to Twitter or Facebook to recommend a product, or report problems and get their issues into the public domain. Keeping customers up to date on social media will, therefore, enhance a company’s reputation for openness.

However, this form of communication also raises questions as to whether social media has changed the responsibilities of companies in informing customers about various issues. Clients expect early disclosure as it is now so easy to place something in the public domain. But passing on bad news can impact on business confidence, and companies may consider it to be too great a risk to publicise the problems, even though failing to do so could result in serious consequences for brand loyalty.

Despite these risks, companies do use social media to announce or comment on incidents affecting customers. These can range from issuing notices about a product recall – see for instance Tesco’s warning about some grated cheese[[2]](#endnote-2) – to reporting an environmental disaster. An interesting, relatively early example of problems surrounding this was seen on Twitter in 2010, following the oil spill from BP’s *Deepwater Horizon* in the Gulf of Mexico. While the company’s official account had 15,000 followers at the time, a parody account had amassed more than 175,000, and was tweeting spoof messages such as “*We are doing everything we can to stop the information leaks in the gulf: http://ow.ly/22XTw #bpcares*”.[[3]](#endnote-3) As parody accounts are allowed on Twitter, there was little BP could do to stop these messages from going out and being shared: they simply had to keep an eye on them and redouble their PR efforts on both social media and in the press.

A more recent example of a well-known company using social media to announce a security incident emerged in the UK in May 2020, when EasyJet posted a statement on its Twitter account announcing that hackers had accessed the email and travel information of around nine million customers, including the credit card details of some 2,000 of them, in a “highly sophisticated attack”.[[4]](#endnote-4)

This led to questions from customers about the data breach, allowing the company to respond quickly to the concerns, and demonstrating transparency over the incident. However, it also invited comments and questions about the length of time EasyJet had taken to tell customers about the breach: despite having informed the Information Commissioner’s Office within 72 hours, as required by the General Data Protection Regulation (GDPR), it appears the incident actually occurred in January - five months before the news hit the media.[[5]](#endnote-5)

*Targeting the audience: some guidelines*

Social media users will have a number of reasons for following company accounts on sites such as Twitter, Facebook or Instagram, be it brand loyalty, more information about products or services, or making a complaint and ensuring their comments are read by other people. LinkedIn, on the other hand, is designed specifically for professional career purposes. Users will follow organisations with which they are interested in building links or working for, and also to develop a network of contacts in their sector, or in one they might hope to join.

Given that the audiences on various social media sites are different, your posts should vary across platforms. Share content as widely as possible, but tailor it according to the needs of the reader.

For example, if you are aiming to attract professional interest, use LinkedIn for business interaction and insights. If you are hoping to quickly publicise a new product or service, post on Twitter in the first instance, as it is best deployed for short, incisive messages aimed at gathering awareness about a particular topic. Facebook is more suited to longer content which can include graphics.

When monitoring the use of your company’s social media accounts, be aware that comments may be posted that will not show up on your timeline. On Twitter it can make a huge difference looking at mentions rather than just replies to your original posts. Taking EasyJet as the example again, it is possible to search for and access many comments about the data breach referred to above which do not show up as replies on their thread announcing the incident. Some people have simply typed in their own comments without tagging EasyJet specifically, yet naming the airline. This illustrates the need for a specific team to take charge of company accounts and to run regular searches for any relevant posts.

Take the social media aspect of your business seriously and check accounts regularly. Appoint a small team of employees who are responsible for creating content and maintaining presence on the networks, as well as responding to comments. This will work far better than an ad hoc approach where someone will quickly log onto Twitter to post a link to a blog, or paste a media story on Facebook.

While it is of course useful to share content from news sites or other business websites, try to focus on publishing original information. For example, webcasts are excellent for personalising content on a YouTube channel. Keep webinars brief and to the point: those people who are interested in viewing or listening do not want to hear a couple of individuals having a chat over coffee. Content should be relevant, incisive and to the point.

Answer questions from customers quickly: if this is not possible due to volume, post a clear message. Never insult people who comment on your accounts: they could be prospective clients. Do not respond to abusive posts made by someone with an agenda – whether business or political.

Remember too that quality matters more than quantity. Ensure your posts are read carefully before being posted. Spelling and grammatical errors reflect poorly on a company’s image. Do not give in to the temptation to post too much. Your target audience may well lose interest if they see your company name popping up too frequently, and they might begin to ignore the updates or stop following you altogether.

*The limits of social media: personal accounts*

While the purpose of this paper is not to highlight the well-publicised incidents that have taken place recently involving the use or sale of personal data (for example, Cambridge Analytica and Facebook[[6]](#endnote-6)), it is worth remembering that nothing is private anymore.

One of the problems here is that many people do not understand that posts they make on social media are essentially open to public view: even if their privacy settings are as strict as possible, it cannot be guaranteed that posts will remain private. There is nothing to stop someone with access to that account from sharing the information posted on it, such as by copying pictures posted by friends on personal pages or in WhatsApp chat groups. Can we all be certain that the people who can view our posts are as responsible with their privacy settings as we are?

For businesses, difficulties can also arise when a member of staff either shares company information on their private accounts inappropriately, or goes so far as to criticise their employer openly. Who knows if a friend or other contact is sharing that post or taking a screenshot of it and then having it read by a competitor?

This highlights the need for employees to exercise caution when making any posts on social media or sharing homemade videos. While they may feel their social and work lives are separate, this is not the case, as has been shown by a range of well-publicised incidents. One of these involved a Canadian rail worker, who was fired after her employer found “racy” pictures of her, apparently taken on company property. She had also made critical posts about her employer. Questions arose over whether she should have been monitored more closely, as she had previously been fired and reinstated (though for different reasons).[[7]](#endnote-7)

However, this leads on to a debate concerning personal responsibility. Should a company be expected to police the online behaviour of its employees to protect them from making poorly thought-out posts? Is it not better to have a strong social media policy in place, stipulating exactly what a member of staff may and may not do on social media in the eyes of their employer?

An example of a company with exactly such a policy involved a junior marketing executive who was excited to be included in a new client pitch, and thrilled when her company was awarded the contract – so thrilled that she posted a picture of the celebratory party to Instagram, with the logo of the new client in plain view. She was dismissed: her company had a clear policy in place and had repeatedly made it clear that social media posts made before any formal announcement of the contract would be a direct violation of her employment contract.[[8]](#endnote-8)

*Using the corporate account*

The use of corporate social media accounts raises a number of often controversial issues. All staff with access to such accounts must of course operate them according to clear company guidelines. Unfortunately, there will always be cases of employees who will use those accounts for their own purposes. For example, someone with a grudge against their employer might take advantage of contacts to build up a list of their own for various reasons, perhaps to work towards obtaining a new job with a rival organisation, or even to embarrass their current employer in some way. In extreme cases they may even be involved in criminal activities. A 2019 Verizon analysis of 40,000 incidents found “more than a third of data breaches involve internal actors”.[[9]](#endnote-9) Of course, this rarely involves the use of corporate social media accounts. An employee who is intent on stealing company data will do so anyway if they are presented with the opportunity. Intellectual property theft is of increasing concern, as is industrial espionage carried out for rival companies or foreign governments.

One other point here concerns the issue of social media being used as a vector for conspiracy theories. At first glance that may appear to be of little importance to workplace social media. However, bear in mind that the latest ‘theory’ consists of allegations that 5G is behind the coronavirus (COVID-19) pandemic. This could have a detrimental impact on companies involved in the telecommunications sector, were 5G conspiracy posts shared on their social media accounts. Similarly, the furore over President Trump’s pronouncements on his use of the anti-malaria drug hydroxychloroquine (and even his disinfectant gaff) could inspire people to target pharmaceutical companies and health facilities.

*Phishing, OSINT and social media*

Social media offers a particularly rich source of data for phishing gangs, whether typical cybercrime groups or hostile state-sponsored APTs aiming to steal corporate information. According to research carried out by KnowBe4, 91% of successful data breaches start with a phishing attack. Further, it was found that LinkedIn is increasingly being used by cybercriminals who exploit the information openly available on the platform to trick employees into clicking on phishing emails. KnowBe4 notes that this is significant because many LinkedIn users, particularly those with business development responsibilities, have their accounts linked to their corporate email addresses: this increases the risk of a phishing attack, or other social-engineering related threat.[[10]](#endnote-10)

Phishing scams involve launching targeted attacks against a company or an individual. They are likely to begin with a threat actor gathering intelligence on the target by scanning open source intelligence (OSINT). They might run searches on media or genealogy websites, or they may look for more specific information available from organisations such as Companies House, in telephone directories and the electoral roll, and on social media. Publicly accessible information can offer a wealth of data - in many cases enough to provide a threat actor with everything they need to profile an individual or an organisation. From there the attackers will hope to establish contacts in their preparations for a targeted attack.

These are common social engineering research techniques that are used by cybercriminals and state-sponsored APTs alike: they have even been deployed in military settings. One recent example was highlighted in February 2020, when the Israel Defense Force (IDF) and Israel Security Agency (ISA) were targeted in a Hamas operation using fake social media accounts to hack soldiers’ phones. A Hamas operator would pose as an attractive young woman on social media and urge the soldiers to download a dating app disguising a Mobile Remote Access Trojan (MRAT). Hackers were then able to harvest information about the victim, including phone numbers, locations and SMS messages.[[11]](#endnote-11)

*Business Email Compromise*

The FBI’s Internet Crime Complaint Center (IC3) reported in 2019 that it had received 23,775 Business Email Compromise (BEC) complaints, with adjusted losses of over $1.7 billion. An increase in scams specifically targeting payroll funds was also noted.[[12]](#endnote-12)

Attackers focusing on this highly lucrative scam are likely to spend a great deal of time - possibly months - researching and monitoring their victims. To launch a successful attack, the cybercriminal will need to know enough about the organisation to be able to pose as a senior executive with the ability to authorise large payments. As with the traditional phishing scam, the first step in the attack will involve gathering intelligence on the target company by scanning OSINT, locating media articles featuring the enterprise, or following social media accounts. They may then use social engineering techniques to build up a relationship with employees, such as by posing as a professional involved in the same business sector. LinkedIn accounts provide an excellent source of information for this type of fraudster.

A classic example of BEC took place in January 2016, when Austrian aeronautics company Fischer Advanced Composite Components AG (FACC) was duped into wiring some €50 million to cybercriminals.[[13]](#endnote-13) CEO Walter Stephan was later fired. Many similar, high-profile BEC scams have been reported in recent years.

In 2019 the Argentinian football team Boca Juniors discovered that a transaction worth €520,000 had been stolen. Following the transfer of Leandro Paredes from FC Zenit to Paris Saint-Germain FC, Boca Juniors was set to receive part of the payment, which was split into three instalments. The first of these was intercepted in a BEC scam after the hacker gained access to the details in an employee's email account.[[14]](#endnote-14)

One recent and highly successful scam came to light in May 2020, when hackers managed to steal $10 million from Norfund, a private equity company owned by the Norwegian Ministry of Foreign Affairs and funded by the state budget. The cybercriminals gained access to the Norfund email system, where they carefully monitored employee communication for several months. After they had identified the staff member responsible for managing transactions, they created a Norfund email address impersonating an employee who was able to authorise fund transfers. Using this email address, they altered the payment information for an investment destined for a Cambodian financial institution, so that the money was transferred instead to a Mexican bank account. The threat actors then attempted to prevent the discovery of their operation by emailing the Cambodian financial institution and stating that the transaction would be delayed due to the spread of COVID-19 in Norway. This move was important, as it provided them with valuable time to physically cash out the stolen funds.[[15]](#endnote-15)

Importantly, the emails used in these campaigns will not contain malicious links or attachments and they are therefore less easy to spot. On the other hand, the solution to thwarting such attacks is relatively simple: as well as ensuring that two-factor authentication (2FA) is implemented on all company email accounts, insist on verbal confirmation - preferably face-to-face - from a colleague who has the authority to approve large financial transactions before any payments are sent. This call should come from the recipient of the email, rather than the sender, to further ensure its validity.

*COVID-19*

COVID-19 offers an excellent opportunity for both state-sponsored hacker groups and cybercriminal fraud gangs. In recent months, the pandemic has featured in a wide range of scams and attacks. **At the end of May, for instance, the UK’s Actionfraud team reported that 2,057 victims in the country had lost a combined total of over £4.6m to scams related to COVID-19.**[[16]](#endnote-16)

Earlier in the same month, Palo Alto detailed the activities of Nigerian cybercriminal group SilverTerrier, which had been launching COVID-19-themed phishing campaigns in attempts to compromise victims. The most prominent effort relied on exploiting vulnerabilities to deliver infostealer malware such as Formbook, Lokibot and Agent Tesla. Targets included health departments worldwide. None of the attacks were thought to have been successful.[[17]](#endnote-17)

Other common scams have involved emails purporting to come from the director-general of the World Health Organisation (WHO), or companies offering facemasks and other PPE supplies. The US Health and Human Services Department was hit by a cyber-attack on its computer systems[[18]](#endnote-18) and in March *Reuters* reported that the Iranian government had targeted the WHO by attempting to hack into the email accounts of staff.[[19]](#endnote-19)

Added to this is the concern about state-sponsored hacker groups from Russia, Iran and China, which are believed to have been attempting to access and steal vital medical research from institutions working on the development of a COVID-19 vaccine, such as the University of Oxford.[[20]](#endnote-20)

The UK’s National Cyber Security Centre (NSCS) and the US Department of Homeland Security’s (DHS) Cybersecurity and Infrastructure Security Agency (CISA) issued a joint alert[[21]](#endnote-21) about the dangers of cybercriminal groups and state-sponsored APTs taking advantage of the pandemic to target businesses and individuals with COVID-19-related phishing scams. They warned that the increase in the number of employees working at home was “amplifying” the threat posed by malicious actors.

Echoing these concerns, the *Financial Times* quoted James Lewis, a cybersecurity expert from Washington’s Center for Strategic and International Studies, who said: “Work from home is a gold mine for spies. The Chinese in particular benefit because it gives them more and easier targets to go after and they have the resources to take advantage of a surge in easier targets.” The “rapid” move to home working meant that well-known weaknesses in VPNs and other remote working software were being exploited, Lewis added, noting that hackers would need to have done “a little advance work” by linking home network addresses to targeted individuals, and that “they will try to implant malware intended to stay after lockdowns have ended”.[[22]](#endnote-22)

This “advance work” will certainly involve some research on social media sites, particularly LinkedIn, illustrating the dangers of linking home and work email addresses. The responsible use of social media is, therefore, likely to assume even more importance post-COVID, as working practices change to allow more people to work from home in environments with less oversight.

*Addressing the risks: staff training and policies*

Regular cybersecurity training should be mandatoryfor all staff, from the post room to the boardroom. It should include specific sessions on the use of social media. Phishing simulation exercises to test employee awareness can also be very useful. However, it is important to note that nobody can be expected to spot a dubious email or link all the time: mistakes will happen. The overall cybersecurity measures in place in the organisation are of greater importance. It is no use blaming an employee for clicking on a malicious link if software has not been updated, known vulnerabilities have not been patched, and data has not been fully backed-up.

One useful training method is to require employees to run a digital footprint exercise on themselves: ask them to find out what parts of their social media presence are open to public view. Such an exercise does not simply entail clicking on a Facebook page and adjusting the privacy settings: friends’ lists should be assessed, and their accounts appraised to see what sort of information they are sharing. For example, a staff member might find that their parent or friend has an account with fairly lax privacy protocols, and they could be posting pictures of the employee in question or details about grandchildren, hobbies and more.

Websites listing public information should also be examined. Children’s names can be discovered, and searches made for their own social media accounts, where a great deal of information might be available, possibly even enough to pose a security threat to the family. One other thing to bear in mind here is that a child’s name may offer a clue to hackers about passwords used by parents: ensure that all training sessions also include information about basic password security, including the use of a different password for each of their accounts.

This paper has focused on the use of social media within organisations. Allied to this, Ian Thornton-Trump and Zoë Rose have previously outlined the benefits of a dedicated team of individuals in charge of a company’s OSINT activities which could save the organisation from reputational damage. This team should look for the following:

*• Counterfeit or stolen property listed online*

*• Employee conduct, threats and harassment on social media*

*• Frustrated, angry or threatening customer correspondence*

*• Damaging reviews of product, services or work environment*

*• Leaked merger, acquisition & organizational partnership discussions*

*• Sensitive information publicly disclosed – accidentally or intentionally*

*• Inaccurate, harmful or out of date information*

*• Presence of fake websites, fake invoices or scams targeting customers, staff or the organization*

*• Staff disputes, associations or controversial commentary in a public forum*

*• Credentials from data breach & compromised accounts belonging to the organization*

*• Research and validation of the background of prospective employees or board members*

*• Unsavory relationships, membership or pending court action related to the organization*

They conclude that a well thought-out OSINT programme “will build intelligence and give recommendations, resilience prevention, detection and responses”, allowing senior staff to “either directly take action or advise on actions to be taken, both in response and future prevention, via keeping in mind considerations like implementing more robust acceptable use policies, training, active monitoring and controls”.[[23]](#endnote-23)

*Recommendations*

Develop a specific social media policy for all employees with clear guidance on the posting of both personal and corporate information.

Organise regular training sessions on cybersecurity for all employees and include a focus on the use of social media, with particular reference to the dangers posed by phishing scams.

Ensure 2FA is used for all company email accounts.

Identify a small team of individuals to be tasked with the operation of your organisation’s social media accounts. Set out detailed lines of responsibility and accountability, and ensure people know exactly what their role entails.

Read your contributions carefully before posting them and tailor content according to the platform and audience. Quality matters more than quantity.

Check your account notifications regularly.

Respond to comments in a timely manner. Be communicative and helpful.

*And finally, one last warning about social media:* *in May 2020 a Cyjax researcher found that Greg Clark MP had broadcast his mobile phone number on a BBC Facetime interview[[24]](#endnote-24). Be aware of the information you are sharing when participating in such sessions*.

June 2020

Terry Mayer BA (Hons), MSc

Published by Cyjax Ltd., London

1. https://www.socialmediatoday.com/news/8-social-media-marketing-stats-you-shouldnt-ignore/557405 [↑](#endnote-ref-1)
2. https://twitter.com/Tesco/status/1141024527968886784 [↑](#endnote-ref-2)
3. <https://techcrunch.com/2010/06/26/bp-pr-bpglobalpr/> [↑](#endnote-ref-3)
4. https://twitter.com/easyJet/status/1262802432872120321 [↑](#endnote-ref-4)
5. <https://www.independent.co.uk/life-style/gadgets-and-tech/news/easyjet-cyber-attack-hack-personal-data-credit-card-details-a9523731.html> [↑](#endnote-ref-5)
6. https://www.wired.com/story/cambridge-analytica-facebook-privacy-awakening/ [↑](#endnote-ref-6)
7. <https://www.tripwire.com/state-of-security/risk-based-security-for-executives/connecting-security-to-the-business/osint-using-threat-intelligence-secure-organisation/> [↑](#endnote-ref-7)
8. https://thefinancialdiet.com/financial-confessions-lost-job-social-media-post [↑](#endnote-ref-8)
9. https://enterprise.verizon.com/en-gb/resources/reports/insider-threat-report/ [↑](#endnote-ref-9)
10. https://www.channelfutures.com/mssp-insider/knowbe4-cybercriminals-setting-linkedin-phishing-traps [↑](#endnote-ref-10)
11. https://research.checkpoint.com/2020/hamas-android-malware-on-idf-soldiers-this-is-how-it-happened [↑](#endnote-ref-11)
12. https://pdf.ic3.gov/2019\_IC3Report.pdf [↑](#endnote-ref-12)
13. https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/austrian-aeronautics-company-loses-42m-to-bec-scam [↑](#endnote-ref-13)
14. <https://mundohacker.net.br/hackers-roubam-500-mil-euros-do-time-de-futebol-boca-juniors/> [↑](#endnote-ref-14)
15. <https://securityaffairs.co/wordpress/103242/cyber-crime/norway-norfund-scam.html> [↑](#endnote-ref-15)
16. <https://www.actionfraud.police.uk/covid19> [↑](#endnote-ref-16)
17. https://unit42.paloaltonetworks.com/silverterrier-covid-19-themed-business-email-compromise [↑](#endnote-ref-17)
18. https://www.bloomberg.com/news/articles/2020-03-16/u-s-health-agency-suffers-cyber-attack-during-covid-19-response [↑](#endnote-ref-18)
19. https://uk.reuters.com/article/uk-health-coronavirus-cyber-iran-exclusi/exclusive-hackers-linked-to-iran-target-who-staff-emails-during-coronavirus-sources-idUKKBN21K1RL [↑](#endnote-ref-19)
20. https://www.zdnet.com/article/hackers-are-targeting-uk-universities-to-steal-coronavirus-research-ncsc-warns [↑](#endnote-ref-20)
21. https://www.ncsc.gov.uk/news/covid-19-exploited-by-cyber-actors-advisory [↑](#endnote-ref-21)
22. https://www.ft.com/content/37149106-eb16-4b4e-879b-2913b99da84f [↑](#endnote-ref-22)
23. <https://www.tripwire.com/state-of-security/risk-based-security-for-executives/connecting-security-to-the-business/osint-using-threat-intelligence-secure-organisation/> [↑](#endnote-ref-23)
24. https://twitter.com/olihough86/status/1262664210993033216 [↑](#endnote-ref-24)