BMJ Health & Care Informatics

Phishing in healthcare organisations: threats, mitigation and approaches

Ward Priestman, Tony Anstis, Isabel G Sebire, Shankar Sridharan, Neil J Sebire

To cite: Priestman W, Anstis T, Sebire IG, *et al*. Phishing in healthcare organisations: threats, mitigation and approaches. *BMJ Health Care Inform* 2019;**26**:e100031. doi:10.1136/bmjhci-2019-100031

Received 28 April 2019
Revised 15 August 2019
Accepted 22 August 2019

DRIVE (Digital Research, Informatics and Virtual Environments), Great Ormond Street Hospital for Children / NIHR GOSH BRC, London, UK

Correspondence to
Professor Neil J Sebire;
neil.sebire@gosh.nhs.uk

ABSTRACT

Introduction Healthcare data have significant value as a potential target for hackers. Phishing is a method of exploitation for malicious reasons using targeted communications (email/messaging). This study reports on an internal evaluation targeting hospital staff and summarises peer-reviewed literature regarding phishing and healthcare.

Methods An assessment was performed as part of cybersecurity activity during a designated test period using multiple credential harvesting approaches through staff email. We also searched the medical-related literature to identify relevant phishing-related publications.

Results During the 1-month testing period, the organisation received 858 200 emails: 139 400 (16%) marketing, 18 871 (2%) identified as potential threats. Of 143 million internet transactions, around 5 million (3%) were suspected threats. 468 employee email addresses were identified from public data and targeted through phishing using a range of payloads including attachments and malicious links; however, no credentials were recovered or malicious files downloaded. Several hospital employees were, however, identified on social media profiles, including some tricked into accepting false friend requests.

Discussion Healthcare organisations are increasingly moving to digital systems, but healthcare professionals have limited awareness of threats. Increasing emphasis on 'cyberhygiene' and information governance through mandatory training increases understanding of these risks. While no credentials were harvested in this study, since up to 5% of emails/internet traffic are suspicious, the need for robust firewalls, cybersecurity infrastructure, IT policies and, most importantly of all, staff training, is emphasised.

Conclusion Hospitals receive a significant volume of potentially malicious emails. While many staff appear to be aware of phishing and respond appropriately, ongoing education is required across the spectrum of cybersecurity, with specific emphasis around 'leakage' of information on social media.

Summary

What is already known?

- Phishing is a method of attempting to gain usernames, passwords or medical data, for malicious reasons, using communications such as email or messaging by encouraging recipients to click links to websites running malicious code or to download or install malware.
- Phishing is increasingly targeting healthcare organisations, but the scale of threat and awareness of staff remains largely undetermined.

What does this paper add?

- 2%–3% of all email and internet traffic to a National Health Service trust was regarded as suspicious/threat, representing >50 million internet transactions and >100 000 emails per annum in one organisation.
- Using a controlled phishing simulation process involving >450 healthcare staff, no credentials were harvested, but the process highlighted potential staff behaviour vulnerabilities that could be exploited by social engineering approaches.
- Healthcare staff education and training represents an important mitigation strategy against ongoing phishing-based cybersecurity threats, which requires ongoing deployment and evaluation.

INTRODUCTION

Healthcare data has significant value and is a potential target for hackers.[1 2] Phishing is a method of attempting to gain potentially valuable details, such as usernames, passwords or medical data, for malicious reasons, using targeted communications such as email or messaging in which the attacking party encourages recipients to click links to websites running malicious code or to download or install malware. Since phishing typically requires the recipient to perform an action, it relies on social engineering techniques, with many contacts therefore appearing to be from trusted sites such as financial institutions, or in the case of healthcare data, IT administrators or healthcare staff.

Phishing refers to this general approach, in which large numbers of untargeted communications are sent to a wide range of recipients in the hope that a minority will become victims. Variants include spear phishing, in which communications are directed at specific individuals, or types of individuals or companies; clone phishing, in which a legitimate email has content changed to create a cloned email containing malicious content; and whaling, in which communications are targeted specifically at senior high-profile

targets, often supposedly originating from 'C-suite' or legal departments.[3 4]

The aim of this study is to report on an internal investigation into phishing targeting healthcare staff at one institution representing a UK National Health Service (NHS) hospital and review the medical peer-reviewed literature regarding phishing affecting healthcare organisations.

METHODS

A detailed local cybersecurity audit was performed by our organisation using a commissioned party along with standard penetration testing approaches as part of routine cybersecurity policy activity. Specific details of the methods and detailed findings of potential vulnerabilities are not provided for obvious reasons, but an overview of the strategy used is provided below.

In general, vulnerability testing was performed during a designated test period, using multiple credential harvesting approaches, including malicious macros, object linking and embedding (OLE) and other payloads in emails to convince employees to access a fake sharepoint/dropbox service to download files, bypassing external restrictions and exploiting commonly misconfigured windows services, outbound firewall rules and simple mail transfer protocol (SMTP) services. Emails were sent from both spoofed and legitimate email providers (used to bypass restrictions on spoofed emails). Since phishing attacks often rely on correctly formatted internal email addresses and information regarding employees names and positions, the structure of the internal email address was obtained using standard web searches. and targets were identified using freely available sources such as Facebook, LinkedIn and Google searches. Furthermore, online dating sites were searched for connections to the organisation, and leaked information from widely published security breaches (such as Adobe, Yahoo! and so on) were used to acquire password and username lists. Employee email addresses identifiable from publicly available scraped data were targeted to accept 'friend requests' from a 'fake' account specifically used for this study.

Armed with the potential internal email addresses discovered during the reconnaissance stage, Microsoft Outlook Web Application was selected to replicate a target that is typically used by threats during a phishing campaign. A domain name similar to the hospital external domain name was setup, and emails were sent to half of the collected email accounts on a weekday morning. The emails contained copied disclaimers, internal formatting and a cloned signature in order to feign authenticity. Any user that clicked on the hyperlink in the email resulted in their web browser redirecting to a fake login page, which attempted to trick users to authenticate (anyone actually submitting their authentication credentials would be sending them to a controlled managed server). Another email was also sent to a subset of employees to attempt to trick them into clicking a fileshare hyperlink. Any user that clicked on the SharePoint hyperlink would also be redirected to a page in which a document could be downloaded and opened and prompted to enable macros. Internal employees were also targeted with a number of emails each containing different potential payloads as batch files obfuscated as embedded objects (eg, a Microsoft Word or Excel file). An attempt was also made to trick employees into believing their Facebook password had been recently changed from a location in China; if clicking on the hyperlink, their browser would redirect to a fake authentication page. A further subset of employees were sent an email purporting to be from a recruitment firm advertising potential employment positions, with embedded documents appearing to be PDF and excel files but representing batch files to call PowerShell and start a download process required to gain access remotely to the employee's computer. No 'whale-phishing' or targeted 'spear-phishing' of preselected individuals was performed as part of this study.

In addition to the internal process, we also performed a search of the medical-related literature using PubMed (all languages, all years) with the search term 'phish*' (21 April 2019) to identify all relevant healthcare phishing-related publications in the academic corpus.

Table 1 Summary of threat message activity during a 1-month period

Threat message summary	%	Messages
Stopped as invalid recipients	0.2	2312
Spam detected	1	9147
Virus detected	0.2	1756
Stopped by content filter	0.5	3974
Stopped by DMARC	0.2	1682
Total threat messages		18871

DMARC, Domain-based Message Authentication, Reporting and Conformance.

Table 2 Internet traffic threat summary during a 1-month period

Suspected transactions summary	%	Number of transactions
Blocked or warned by URL	87.4	4.2 million
Blocked by web reputation	2.4	189 900
Other blocked transactions	10.1	326 500
Total blocked transactions		4.7 million

RESULTS

During the 1-month testing period during a period in 2018, the organisation received 858200 email messages: 139400 (16.2%) were classed as marketing by spam detection systems in place and 18871 (2.2%) identified as potential threats (table 1). In terms of internet traffic, during the reporting period, there were in total

142.7 million transactions of which 4.7 million (2.9%) were suspect (table 2). Using our security infrastructure, emails are flagged as suspicious/malicious based on a combination of known identified subjects, content (including key words), senders or email address, attached file names or file SHA256 Hash values. The system uses a combination of the above to determine whether the email passes through or is discarded based on a series of rules and policies, some of which are downloaded by a provider and others from manual input derived from news articles, alerts, social media and so on to enhance its operation and compliment the automated ones supplied. False positives/negatives can be overcome by manually updating the rules that govern the passage of messages through the system.

Four hundred and sixty-eight individual employee email addresses were identifiable from publicly scraped data and were targeted. However, during the testing period, no credentials were recovered from the cloned service, no credentials were recovered or files downloaded from the SharePoint cloned service and no credentials were collected from the attempted universal naming convention (UNC) exploitation, indicating that correct outbound firewall policies were in place. During the testing period, either no users believed the authenticity of targeted emails or these were blocked by a perimeter security policy, and no OLE or macro payloads were successfully activated, either through recognition by users or blocking by security policies.

However, we were also able to identify hospital employees, in uniform with identification badges clearly viable, on dating site profile pictures, and four employees were tricked into accepting false friend requests from fictitious profiles on Facebook, including one who replied with a message.

Through the PubMed search, in total, 70 potential papers were initially identified but following review of the titles and abstracts, only 11 were relevant to this area and all are included in the manuscript, including the Discussion and Reference list.

DISCUSSION

With improvements in cross-industry organisational cyber security hardware, software and policies, there is increasing use of targeted email communication (phishing) by potentially malicious persons. Healthcare organisations are increasingly moving to electronic patient record (EPR) systems and other digital systems,[5] but healthcare professionals may have limited awareness of such threats, since most healthcare staff IT training focuses on 'functional' features of the software and applications. Recently, increasing emphasis on 'cyberhygiene' and information governance issues through mandatory training has raised the understanding of these risks. For example, the National Cyber Security Centre provides information regarding basic principles of how organisations can protect themselves from cyber threats including advice in areas such as securing internet connections, devices, controlled access, software patching and data access.[6] The findings from this small targeted study demonstrated that, on this occasion, no credentials were harvested through any of the phishing approaches but highlights that around 2%–3% of the large volume of emails and internet traffic to an NHS Healthcare Organisation are considered suspicious, emphasising the need for robust firewalls, cyber security infrastructure and IT policies and staff training. Since many phishing emails are links to malicious websites and their files, firewalls act as one layer that may be used to block access to these sites and the files. A recent report found that phishing resulted in more breaches than malware and unpatched systems combined (48% vs 41%),[7] especially true of staff who maybe using personal devices for remote working (which may be un patched and therefore more vulnerable to malware through a phishing link), and again robust firewalls and infrastructure may mitigate some of this risk by restricting access to corporate system even if devices are compromised. In addition, it has been reported that there has been recent increasing use of a variant known as CEO Phishing, in which spoof emails are sent impersonating the company CEO, accounting for almost half of phishing scam emails in some reports,[8] and it is possible that more 'click-throughs' may have occurred if such tactics had also been deployed. Other reports highlight less targeting recently of senior management roles but a large increase in email spoofing of organisations, highlighting the need for controls such as Domain-based Message Authentication, Reporting and Conformance (DMARC).[9 10]

With the move to widespread comprehensive EPR systems and digital storage of novel information types, such as whole genome screening and drug prescribing information, the potential value of health data is likely to increase and increasing sophisticated methods of gaining access are likely. In general, as encryption and technical aspects of cybersecurity increase, the 'weak link' increasingly becomes the human users, with manipulation and social engineering becoming relatively more important.[11] Several recent healthcare specific data breaches through phishing have now been reported including Augusta University Health, exposing >400 000 records.[12] There are of course many ways that data breaches may occur other than phishing, but according to the most recent Verizon report, around 40% of malware across all organisations is delivered by email, with overall 'click rates' of around 3%; phishing now accounting for more than 80% of social hacking.[13] With increasing perimeter protection and sophistication of automated systems to detect suspicious communications, in relative terms, the risk for any organisation therefore increasingly becomes its staff, in terms of behaviour and vulnerability to social engineering. In every case where a phishing attack has been successful, there is a human action through social engineering, using psychological manipulation of people into performing actions or divulging confidential information.

Various methods have been previously described to try and identify most vulnerable users of a system, including signal detection theory, evaluation of proportion of risk attributable to the most vulnerable users or evaluation of results from random versus spear phishing. In general, more vulnerable users are less cautious regarding all links and attachments and less able to distinguish phishing from legitimate emails; tests to identify such individuals so they can have targeted behavioural interventions are therefore important, and 'return on investment' for such users has greater benefit than blanket deployment of standard approaches.[14] However, performing 'testing', such as the current study, phishing experiments raises various issues regarding staff consent since, by definition, the process requires deception. However, it is generally accepted that such approaches are ethical providing that risks are minimised, the user's confidentiality and privacy are protected and the learning provides feedback for the common good.[15]

To determine whether demographic factors may be related to phishing vulnerability, one study recruited around 200 participants, including approximately equal numbers of younger and older adults, and logistic regression analysis revealed three statistically significant predictors of phishing risk, namely, education level, preexisting awareness of phishing and performance on neuropsychological assessment tests, suggesting that relatively simple educational interventions could be effective in reducing phishing vulnerability.[16] Technical tools may improve detection rates, but lack of knowledge of 'risk clues' appears of most importance in terms of reducing 'click-through' rates. For example, in one study, the presence of cues such as domain highlighting allowed participants to distinguish legitimate versus fraudulent websites better than baseline, but there remained failure to detect many fraudulent web pages, indicating that many users simply lack knowledge of security cues or how to use these to prevent risk behaviours.[17] Subjects first need to detect whether an email is suspicious for phishing, and then must deal with the email appropriately. Those with greatest likelihood to treat emails as legitimate tend to underestimate the perceived adverse consequences from their actions despite being confident in their own abilities. Providing users with feedback ongoing information about the consequences of phishing could allow targeting of those with the highest risk profiles,[18] and this combination of factors represents the human component of security, which cannot be mitigated by technology alone.[19] In our organisation, we send regular communications informing colleagues how to identify malicious emails, in addition to screensavers, and feedback from 'controlled' phishing studios such as this, so we educate staff by experience.

While some forms of phishing are highly targeted towards specific C-level individuals (eg, 'whale phishing'), results of a cybercrime survey including >10 000 people reported that personal background and financial characteristics in general play little role, with only 'targeted browsing' leading to increased risk. Use of specific operating systems or browsers does not appear to be associated with greater risk, and antivirus software has no effect, further indicating that board training and behavioural prevention are required.[20] It has also been reported that novel antiphishing training in both simple comic and more complex video game forms can reduce phishing susceptibility as measured by rates for all individuals including both students and experienced computing participants.[21]

Two recent studies have specifically reported on aspects of phishing in healthcare organisations in the USA. In the first study, around 5000 employees were targeted by phishing emails, methodologically similar to the present study in that the primary outcome was click-through rates of potentially malicious links/files without further individual targeting through social media, of whom >3500 (65%) clicked on at least two suspicious emails. Importantly, a mandatory training programme did not have any significant effect, with those previously scammed remaining more likely to click on a phishing email, suggesting that targeted staff training may be required.[22] The second paper was a retrospective, multicentre study of six US healthcare institutions that ran phishing simulations from 2011 to 2018 and reported that of around 3 million phishing emails, around 400 000 (14%) were clicked, but in this study, repeated phishing campaigns were associated with reduced odds of clicking on subsequent phishing emails.[23]

General approaches to reduce risk should therefore include both technical and behavioural tactics. Employees should be actively encouraged to question the authenticity of any email that deviates from their standard work, they should consider carefully the sender and context and if in doubt do not open and seek the advice of the organisational security team. All staff should be educated regarding the potential dangers of malicious email attachments and, specifically, staff should never 'verify' any details from an email, click on hyperlinks or open unknown attachments. Users should also be aware of additional methods to confirm that any site linked to is genuine, including various methods of two-factor authentication and use of user-selected images in login pages for legitimate sites. Organisational IT departments should disable functionality that is not required in an employee's daily work, such as Office macros and Windows PowerShell, and run appropriate firewalls with blocked lists of known phishing sites with email spam filters using machine learning approaches.[24] In addition, the increasing use of multifactor authentication may mitigate some risks but itself may have disadvantages in healthcare settings with time-sensitive activities and requires further evaluation for optimal deployment in hospitals.[25]

In addition to random phishing, employees should be aware of the risks of social media activity. For example, despite guidance regarding any use of organisation uniforms in photographs for social media purposes, in the present study, we were able to identify hospital

employees, in full uniform with identification badges clearly viable on dating site profile pictures, and four employees were lured into accepting friend requests from a fictitious profile on Facebook, including one who replied with a message, providing a potential opportunity for further personal information gathering and therefore more sophisticated social engineering attacks, including highly targeted 'spear phishing'. One of the main aims of any phishing attack is often to gain access to a network as an initial step towards a data intrusion. While individuals may be wary of emails containing attachments if they can be accepted to agree to a friend request on a social media site, a subsequent 'trusted' relationship can be built, and subsequently, an attachment may be more likely to be opened when sent from the 'friend'. For example, in a recent 'spear phishing' attack against a US healthcare institution more than 2 million emails were breached.[26] In addition, if a malicious actor can enter an organisation unchallenged, they may be able to find a credentialled computer providing them immediate access to the network. Such intrusion approaches usually require some form of social engineering, and knowledge of specific staff members names and job titles facilitates plausible responses to questioning. Furthermore, public display of security badge is allows spoofing of the external appearance of the badge, even though it may not be functional, which may then be enough to plausibly convince someone to allow tailgating for access to a restricted area. Therefore, social media awareness remains part of a wider security assessment.

The impact of the 2017 WannaCry ransomware across numerous NHS organisations raised the profile regarding need for improved IT security awareness,[27 28] and cybersecurity has now become more prominent across NHS organisations, with requirements for security to be considered at board level and managed as an ongoing board level risk, and coordination of approaches across NHS England and NHS Digital, along with other government cyber security strategies.[29] However, 'phishing' as a search term finds only four results on the NHS Digital website (increased from one result 1 year ago),[30] with advice to 'beware of phishing scams'. NHS Digital provides a cybersecurity support module regarding overall cybersecurity and resiliency, cyber-resilience exercises based on realistic incidents with a 'simulated phishing tool' in association with an NHS-wide national cyber security campaign, a cybersecurity glossary that includes phishing, smishing, spear phishing, whaling, social engineering and cybersecurity advice such as recognition of spelling and grammatical errors, suspicious hyperlinks and care with social media.

The findings of the current study suggest that while many NHS staff appear to be aware of phishing approaches and do not click through potentially malicious links or attachments, ongoing education is required, with specific emphasis required around 'leakage' of information on social media sites, which may allow targeted phishing or other social engineering attacks. As of 2016, more than 70 000 patients had been documented as affected by at least 10 phishing attacks on US Healthcare institutions, and this threat will only increase globally with both increasing volume and scope of digitisation of health information and the potential value of such data for generic crimes such as identify theft and specifically for health data, targeted blackmail, payroll and payer fraud or as a route to ransomware attacks.[31] These factors should therefore influence information security policies on an ongoing basis, both through reiteration of basic security practices such as password policies and regarding developments such as intelligent networking threat detection systems, DMARC email authentication, policy, and reporting protocol implementation, increasing consideration of staff education and training, and on-site and personal device physical security awareness.

Contributors WP and TA contributed to the data collection. SS, ISG and NJS contributed to the manuscript writing, analysis and literature review. All authors contributed to the writing of the final revised manuscript.

Funding The authors have not declared a specific grant for this research from any funding agency in the public, commercial or not-for-profit sectors.

Competing interests None declared.

Patient consent for publication Not required.

Provenance and peer review Not commissioned; externally peer reviewed.

Data availability statement All data relevant to the study are included in the article or uploaded as supplementary information.

REFERENCES

1. Harper EM. The economic value of health care data. *Nurs Adm Q* 2013;37:105–8.
2. Humer C, Finkle J. Your medical record is worth more to hackers than your credit card. Available: https://www.reuters.com/article/us-cybersecurity-hospitals/your-medical-record-is-worth-more-to-hackers-than-your-credit-card-idUSKCN0HJ21I20140924 [Accessed 16 Feb 2018].
3. CSO. Types of phishing attacks and how to identify them. Available: https://www.csoonline.com/article/3234716/phishing/types-of-phishing-attacks-and-how-to-identify-them.html [Accessed 16 Feb 2018].
4. Wikipedia. Phishing, 2018. Available: https://en.wikipedia.org/wiki/Phishing
5. HealthIT.gov. What are the advantages of electronic health records? Available: https://www.healthit.gov/faq/what-are-advantages-electronic-health-records [Accessed 22 Apr 2019].
6. National Cyber Security Centre. Cyber essentials, 2019. Available: https://www.cyberessentials.ncsc.gov.uk/
7. Help Net Security. Phished credentials caused twice as many breaches than malware in the past year. Available: https://www.helpnetsecurity.com/2018/09/13/phished-credentials/ [Accessed 23 Jun 2019].
8. ITProPortal. Fake CEOs appear in nearly half of phishing SCAM emails. Available: https://www.itproportal.com/news/fake-ceos-appear-in-nearly-half-of-phishing-scam-emails/ [Accessed 22 Apr 2019].
9. Proofpoint UK. Protecting people: a quarterly analysis of highly targeted cyber attacks. Available: https://www.proofpoint.com/uk/resources/threat-reports/quarterly-threat-analysis [Accessed 23 Jun 2019].
10. DMARC. dmarc.org – domain message authentication reporting conformance. Available: https://dmarc.org/ [Accessed 23 Jun 2019].

11. Kaspersky Lab US. What is social engineering? | definition. Available: https://usa.kaspersky.com/resource-center/definitions/social-engineering [Accessed 22 Apr 2019].
12. Latest Hacking News. Augusta university health exposed 417K records due to Phishing. Available: https://latesthackingnews.com/2018/08/19/augusta-university-health-exposed-417k-records-due-to-phishing-attacks/ [Accessed 23 Jun 2019].
13. Verizon Enterprise Solutions. 2019 data breach investigations report. Available: https://enterprise.verizon.com/resources/reports/dbir/ [Accessed 23 Jun 2019].
14. Canfield CI, Fischhoff B. Setting priorities in behavioral interventions: an application to reducing Phishing risk. *Risk Anal* 2018;38:826–38.
15. Resnik DB, Finn PR. Ethics and phishing experiments. *Sci Eng Ethics* 2018;24:1241–52.
16. Gavett BE, Zhao R, John SE, *et al*. Phishing suspiciousness in older and younger adults: the role of executive functioning. *PLoS One* 2017;12:e0171620.
17. Xiong A, Proctor RW, Yang W, *et al*. Is domain highlighting actually helpful in identifying Phishing web Pages? *Hum Factors* 2017;59:640–60.
18. Canfield CI, Fischhoff B, Davis A. Quantifying Phishing susceptibility for detection and behavior decisions. *Hum Factors* 2016;58:1158–72.
19. Proctor RW, Chen J. The role of human Factors/Ergonomics in the science of security: decision making and action selection in cyberspace. *Hum Factors* 2015;57:721–7.
20. Leukfeldt ER. Phishing for suitable targets in the Netherlands: routine activity theory and phishing victimization. *Cyberpsychol Behav Soc Netw* 2014;17:551–5.
21. Mayhorn CB, Nyeste PG. Training users to counteract phishing. *Work* 2012;41(Suppl 1):3549–52.
22. Gordon WJ, Wright A, Glynn RJ, *et al*. Evaluation of a mandatory phishing training program for high-risk employees at a US healthcare system. *J Am Med Inform Assoc* 2019;26:547–52.
23. Gordon WJ, Wright A, Aiyagari R, *et al*. Assessment of employee susceptibility to phishing attacks at US health care institutions. *JAMA Netw Open* 2019;2:e190393.
24. NHS Digital. Data security centre. Available: https://digital.nhs.uk/services/data-security-centre [Accessed 22 Apr 2019].
25. HealthTech. Advantages of multi-factor authentication for healthcare organizations. Available: https://healthtechmagazine.net/article/2018/12/benefits-multifactor-authentication-healthcare-perfcon [Accessed 22 Apr 2019].
26. Health IT Security. 350,000 patients, 2M emails exposed in Oregon DHS phishing attack. Available: https://healthitsecurity.com/news/350000-patients-2m-emails-exposed-in-oregon-dhs-phishing-attack [Accessed 22 Apr 2019].
27. Ehrenfeld JM. WannaCry, cybersecurity and health information technology: a time to act. *J Med Syst* 2017;41:104.
28. Martin G, Ghafur S, Kinross J, *et al*. WannaCry-a year on. *BMJ* 2018;361:k2381.
29. NHS England. Cyber security. Available: https://www.england.nhs.uk/digitaltechnology/connecteddigitalsystems/cyber/ [Accessed 02 Jan 2019].
30. NHS Digital. 8 cyber security tips you can start doing right now. Available: https://digital.nhs.uk/blog/transformation-blog/2017/8-cyber-security-tips-you-can-start-doing-right-now [Accessed 02 Jan 2019].
31. Wright A, Aaron S, Bates DW. The big phish: cyberattacks against U.S. healthcare systems. *J Gen Intern Med* 2016;31:1115–8.