WORLD FEDERATION
OF NEUROLOGY

WFN cybercrime policy on phishing attempts

For WFN Staff and Trustees

Version: 08 December 2023 CKM

Content

Preamble

Cybercrime is criminal activity involving computers or digital technology. These include phishing, malware, hacking, identity theft, distributed denial of service, online fraud, and data breach.

This document describes phishing and malware within the context of WFN, and a protocol for handling phishing campaigns targeting WFN staff and trustees, and people working with the organization across its many activities.

Other forms of cybercrime that exist—such as extortion, online intimidation and harassment including trolling, cyberstalking, mobbing, grooming, or abuse—are not covered in this document.

WFN is not responsible or liable for inaccuracies, errors, omissions, or timeliness with respect to the information contained. WFN, its staff, trustees, and its agents are not liable for any damages, including direct, indirect, special, incidental, or consequential damages, or loss of profits arising from or in connection with any action or inability to perform recommendations contained herein and your use of this information is at your own risk.

Malware

Malware is malicious software designed to infiltrate information and communications systems such as computers, mobile devices, and computer networks. Its purpose is to compromise security and steal information for the purpose of selling or committing fraud.

Computer viruses are a type of malware designed to replicate and infect other systems. Its purpose is typically destructive; intended to erase, corrupt, or encrypt data or files.

Common forms of malware

Adware	Profiles and tracks a user's activity on the internet, capturing usage data and personal information without consent. This information is shared or sold to advertisers to enable them to target users with ads. More malicious adware can hijack internet browsers, run remote code, and download malware.
Bots	Autonomous programs used to propagate other malware or internet bots, capable of compromising user accounts, sending spam, and launching attack campaigns.
Keyloggers	Monitors, records, or intercept your keystrokes in order to steal information and account details.
Ransomware	Malware designed to encrypt data, systems, or files, so it is unusable or inaccessible, before demanding a ransom to be paid for decryption.
Rootkits	Gives hackers remote access or control of a computer or device without you knowing.
Spyware	Collects user activity and data such as credit card and banking information, passwords, location etc., without the user's knowledge and sends this to a third party.
Trojans	Malware disguised as desirable code or software such as games, applications, software updates, files, and images.
Worms	Self-replicating malware designed to infect other computers.

Malware is most commonly spread through online downloads, infected storage media such as hard drives and USB drives, malicious attachments and links in email spam, and phishing.

Phishing

"Phishing" is the most common form of cybercrime by which criminals use scam emails, text messages or phone calls to trick their victims into revealing personal, sensitive, or confidential information, and to performing actions that enable cybercriminals to access restricted systems or commit fraud. Phishing is the main delivery method of ransomware, and stolen credentials the most common cause of data breaches.

Phishing uses social engineering—psychological manipulation that exploit and influence human behaviour—to trick victims into making mistakes such as clicking on a bad link, opening an attachment containing malware, disclosing account or security information, and making financial transactions.

Common examples of phishing to look out for:

- You receive a notification for a purchase that you did not make.
- Your account has been suspended or limited.
- Someone has reset your password.
- You have a security alert out of the blue that requires you to verify your ID.
- You receive a notification that suspicious activity has been detected on your computer or account and you must contact a live technician.
- You have a delivery scheduled, stuck in customs, or attempted to be delivered, even though you are not expecting a delivery.
- A hacker has installed spyware onto your computer and has recorded incriminating or degrading videos of you.

Spam and junk email

When we talk about spam email, most people think of it as unsolicited, nuisance email cluttering our inboxes. But spam has more malicious purposes: propagating dangerous links and attachments, baiting unsuspecting or gullible people, and infecting or infiltrating unprotected systems.

Spam *can* be sent by real humans and a lot of spam propagated on social media is from clickbait—content designed to trigger or induce people to share with friends, family, and colleagues, for example fake news presented as fact, or an offer too good to miss. But most spam is generated by botnets, networks of computers running bots and spambots: autonomous programs that can interact with users and systems in online forums and social media platforms, and bulk send spam to harvested profiles. If your computer or device is infected, it is possible it is part of the network generating and propagating spambots!

Spam calls and messaging

Most people are exposed to phishing through spam and junk email, but phishing is also prevalent in social media and messaging platforms such as Facebook, LinkedIn, WhatsApp, and mobile text messaging.

Phishing is widespread through nuisance telephone calls pretending to be from a bank, utility company, internet or IT support company, and other organisations you may have heard of or are familiar with.

The general recommendation is:

Do not react or reply before you are able to confirm the authenticity of the sender's email address or telephone number.

Do not click on any links or open any attachments that you are not expecting. If you are unsure, check with your company's IT department if you have one, or with someone you know who may be able to advise.

If you receive a telephone cold call, the best thing to do is hang up immediately and report the number to the agency or regulatory body in your country if one exists. In the UK[1] and US[2] you can report any suspicious texts or phone calls to 7726. The number '7726' was chosen because it spells 'SPAM' on an alphanumeric phone keypad. In France it is 33700[3], and in India it is 1909.

[1] Ofcom – UK regulator for the communications services: https://www.ofcom.org.uk/phones-telecoms-and-internet/advice-for-consumers/scams/7726-reporting-scam-texts-and-calls

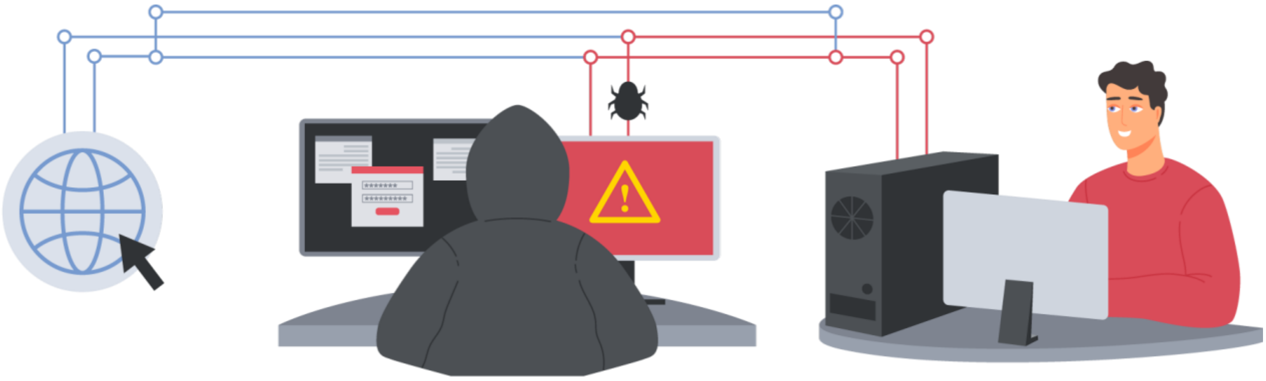
[2] US Federal Trade Commission: https://consumer.ftc.gov/articles/how-recognize-and-report-spam-text-messages

[3] https://www.33700.fr

Fake websites and public wi-fi

Another aspect of phishing is “**pharming**”. This is where cybercriminals redirect users to fraudulent or spoofed websites. In cybercrime, spoofing is where cybercriminals disguise a fake website or online portal, email address or telephone number, to impersonate a trusted or known source or brand. Spoofing is often used in **man-in-the-middle** (MITM) attacks.

MITM attacks are a common form of cyberattack that can occur when people connect to public wi-fi networks, such as those found in coffee shops, airports, and hotels. For example, the hacker may create a network called "CoffeeShopFreeWi-Fi" that looks identical to the real network offered by the coffee shop. When you connect to this fake network, your traffic is routed through the hacker's computer, where they can intercept and read all of your traffic.



You may be redirected to a spoof website where the hacker will eavesdrop or intercept the information you are entering, whilst impersonating you on the actual website. You might receive a call you on your phone from the hacker posing as customer services or IT support from the site you are having trouble accessing or transacting, asking you to validate your login details including one-time-passcodes or 2-factor authentication codes. They may even use reverse psychology to insist you to prove you are who you say you are before they can help you by asking you to click on a validation link, or running a software update to fix connection problems you are experiencing.

Modern cyberthreats and spear phishing

The majority of phishing is generally random; cold calling and targeting curated email lists and telephone numbers. However, “**spear phishing**”, where the criminal does prior research on high value targets such as CEOs and senior executives, is widespread. Attackers employ a targeted approach, building detailed profiles of their victims and crafting personalised phishing strategies that exploit existing trust relationships and appear authentic due to their familiarity and inclusion of accurate details. Unfortunately, these approaches often succeed due to the victim’s carelessness or negligence.

Fuelled by the rapid advancements in artificial intelligence (AI) and machine learning, cybercriminals are increasingly exploiting sophisticated audio-visual "deepfakes" technology—audio-visual synthetic media that can be manipulated to make it appear as if a person is saying or doing something they never did—to target and impersonate senior executives.

The level of realism achieved through deepfakes is so remarkable that even familiar individuals can be fooled into believing the deepfake is the genuine counterpart.

WFN and phishing

It is important that WFN staff and trustees learn to recognise phishing attempts. Here are some real examples of phishing email pretending to be from the President and trustee:

> *Hello Steven, Are you available at the moment? Let me know.*

> *I need you to help me take care of something asap, kindly reply and let me know if you are available.*

> *Hello Richard, How are you? Please can you help the board with something today? Let me know so I can explain better.*

The subject matter is often non-specific and vague. The objective is to enter into a dialogue and establish trust.

When people are busy, in a rush, or are distracted, it is easy to let down our guard and react or respond too quickly without looking at who actually sent the message.

Always try to be vigilant - look out for uncharacteristic use of language (spelling mistakes and poor grammar), unusual salutation, or spoofed email and website addresses. Hackers may use non-Latin Unicode characters such as Cyrillic, Chinese, or Arabic to create addresses that look nearly identical to a real address but direct to someone or someplace else.

For example: the URL wfneurology.org looks legitimate but is not the same as wfneurology.org; in the example the Latin character o has been replaced with a Cyrillic letter o. This trick can be used to spoof email addresses.

Other examples of phishing are aimed at WFN and its online and social media channels. They claim the WFN has violated intellectual property or community standards, and the account will be permanently locked if we if do not respond; or the WFN website domain name is owned by someone else, and we must contact them urgently otherwise the web site will be closed down.

Cybercriminals will use psychological manipulation to trigger people into reacting, and motivate them to respond through:

- Panic
- Anxiety
- Sense of urgency
- Implicit threats
- Gaslighting
- A fear of missing out
- Eliciting sympathy, guilt, goodwill
- Appealing to your sense of duty and obligation.

By manipulating and steering the conversation, cybercriminals try to obtain personal and confidential information or gain access to protected systems, encouraging you to answer security questions or verify authentication codes, click on links, open attachments, or asking you to make payments.

Safeguarding and prevention

WFN is not responsible for safeguarding your personal computer systems or accounts.

If you own or use a computer or mobile device, **install anti-malware software,** and **backup your documents, files, and data regularly**. It is negligent and a false economy to think you will never get targeted or infected, or your hardware will never fail, get stolen or be damaged.

You can be infected with malware without realising—your computer and internet connection slows down or frequently becomes unresponsive, you get unexpected pop-ups, or your internet browser opens to unknown websites, but you shrug these off at the time. Without a robust security, anti-malware, and backup policy in place, regret will be futile.

Block images and remote content in email that spammers use as Web beacons.

Limit your exposure to potential attacks by **avoiding wi-fi connections that aren't password protected**. If you join or log onto public networks or computers, assume your connection is vulnerable to MITM attacks. In this way you will be giving the appropriate level of caution when connected to public access points. Never log onto secure applications or websites such as banking or company networks over such connections if there is no critical need to do so.

Consider using a virtual private network (VPN) to access the internet or remote network. A VPN runs in the background while you are using the internet and encrypts all of your data. All traffic passes through a safe intermediate stage, known as a VPN server, and prevents cybercriminals from intercepting your data. VPNs are not a free service, and you should always go with a reputable VPN provider.

Set up multi-factor authentication (MFA) to your online accounts, and if you are able, use phishing-resistant MFA such as hardware security keys. Basic forms of MFA such as SMS, one-time passcodes and mobile authenticator apps are susceptible to phishing and MITM attacks. Security keys act as an extra barrier to safeguard your accounts from unauthorised access by hackers. Even if a malicious actor manages to steal your username and password, or gains control of your computer or mobile device, they will still be locked out without possessing the physical security key.

Keep your software updated. Software updates are normally released to patch up security holes and deliver bugfixes for security vulnerabilities.

How do you know an email is legitimate and what should you do?

Phishing emails and messages often appear to be from someone you know, a trusted supplier, or member of the organisation.

NEVER SEND MONEY unless you are expecting the email and can verify directly with the sender, they are who they say they are.

All financial transactions from WFN will only ever be handled by the WFN Office. If you receive a request for money from anyone else, call the WFN Office directly on +44 20 3542 1657 or email secretariat@wfneurology.org

Things you should do:

1. Be vigilant and suspect any unexpected communications.
   a. Is the subject matter unexpected or vague, and is it asking you to respond with any degree of urgency?
   b. Is the language and grammar used in the email what you would expect from the sender? For example, how they are greeting you or signing off.
2. Before you act on any information contained in an email, text, or message, carry out some quick checks to confirm the legitimacy of the message.
   a. Do you recognise the sender's email address / telephone number / social media profile?
   b. When you hover over links, is it to a recognisable URL?
   c. When you click on reply to an email, does the email address change from how it appeared in the original message?
3. If you have any reason to doubt the origin of a message, do not reply to the text or message. Instead, contact the sender or their office directly using an existing email address or telephone number you have for them.

If you receive a suspicious text or email:

- **DO NOT REPLY**
- **DO NOT OPEN ANY ATTACHMENTS**
- **DO NOT CLICK ON ANY LINKS**
- **DO NOT INSTALL SOFTWARE OR BROWSER EXTENSIONS OR UPDATES BEFORE YOU HAVE CONTACTED YOUR IT DEPARTYMENT FOR ADVICE**.

Forward the suspicious email **as an attachment** to reportphishing@wfneurology.org – if you do not know how to do this, contact your IT department or the WFN Office for advice.

WFN response protocol for phishing attempts

This Protocol is intended to limit the extent of any damage that may be caused by phishing, and its impact on the organization.

You cannot stop people receiving spam and junk mail or prevent people from being caught out by phishing, and WFN is not responsible for safeguarding, compensating, or putting to right external or third-party complaints that have come about as a result of phishing and subsequent fraud or data loss.

Responsibility for fixing or compensating for actual loss or damage due to fraud resulting from a phishing scam should never be an automatic response or assumption. The exception may be if WFN knowingly or unknowingly provided personal, privileged, or confidential data and which consequently facilitated in the actual fraud or data breach.

WFN may be held accountable If they are notified of a phishing attempt or actual fraud due to phishing—that involves WFN staff, trustees, or agents, or relate to WFN activities—and WFN takes no remedial actions that would mitigate escalation of a phishing campaign and resulting in further actual fraud or criminal actions to succeed.

Should the issue require legal redress, the quick actions of WFN may be used as evidence to demonstrate the WFN took reasonable and measured actions to protect the phishing recipient, the actual victim, and WFN staff and trustees from further damage or detriment, and as soon as WFN was made aware of the fact.

Do not automatically assume the worst-case scenario, or that all reported incidents must have a neat conclusion where everyone feels safer. Whilst WFN has a duty to protect its own systems and train staff to be aware of fraudulent activity, it is everyone's responsibility to be vigilant when receiving email or messaging, and to assess the legitimacy and safety of any content, as well as ensure they have adequate software or hardware protection of their systems and data, whether this is personal or through the companies they work for.

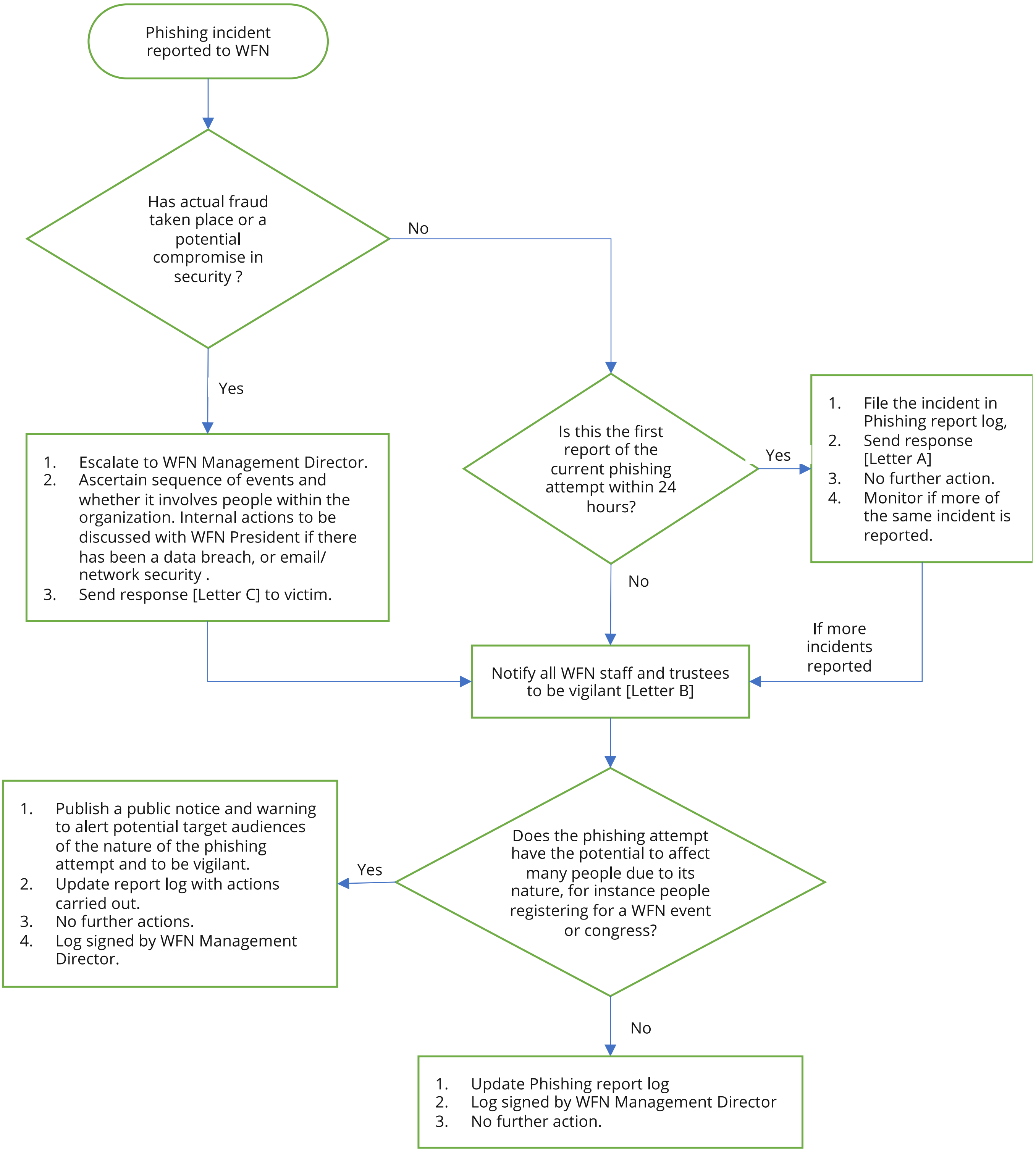
Aside from WFN does not have an IT department responsible for investigating cybercrime and cyberthreats and any actions implementing this protocol falls on the WFN Office, it is generally futile in the case of phishing and spam to try to locate the culprit and to force them to cease and desist. **Spam email generally use spoofed addresses that do not trace back to a real mailbox or trace back to burner accounts that are anonymous.**

If there is actual fraud or evidence of a data breach, this must be escalated to the senior management to agree on what, if any, reparations, or further actions need to be actioned. Depending on the serious nature of the fraud or breach, professional advice should be employed and the incident reported to the relevant authorities.

Response Protocol

Phishing attempts should be reported to report-phishing@wfneurology.org – This address should be made known to WFN staff and trustees.

Email to this address is directed to the WFN Office* who are responsible for assessing the critical nature of the phishing attempt using this protocol.


Phishing incident reported to WFN
Has actual fraud taken place or a potential compromise in security ?
No
Yes
1. Escalate to WFN Management Director.
2. Ascertain sequence of events and whether it involves people within the organization. Internal actions to be discussed with WFN President if there has been a data breach, or email/ network security .
3. Send response [Letter C] to victim.
Is this the first report of the current phishing attempt within 24 hours?
Yes
1. File the incident in Phishing report log,
2. Send response [Letter A]
3. No further action.
4. Monitor if more of the same incident is reported.
No
If more incidents reported
Notify all WFN staff and trustees to be vigilant [Letter B]
Does the phishing attempt have the potential to affect many people due to its nature, for instance people registering for a WFN event or congress?
Yes
1. Publish a public notice and warning to alert potential target audiences of the nature of the phishing attempt and to be vigilant.
2. Update report log with actions carried out.
3. No further actions.
4. Log signed by WFN Management Director.
No
1. Update Phishing report log
2. Log signed by WFN Management Director
3. No further action.

* Mr Carlos Hunte, who is also the designated WFN Data Protection Officer, will be the first point of contact and responsible for carrying out this protocol.

Appendix I - Letter A

Dear [Name],

Thank you for alerting WFN to the suspicious [email] [phone call] [text message] you have received. We can confirm that this did not originate from WFN.

We are currently monitoring reports in case this is a concerted campaign targeting WFN staff, trustees and people working with WFN across our many activities.

[Email: Delete as appropriate]

As with any suspicious email or texts, we recommend you mark as junk and delete from your system.

- **DO NOT REPLY TO THE EMAIL**
- **DO NOT OPEN ANY ATTACHMENTS**. They can contain malicious code that may infect your computer or mobile phone. This includes messages through social media accounts (e.g. Facebook, LinkedIn).
- **DO NOT CLICK ON ANY LINKS**. If you have, we recommend you do a complete scan of your device for malware.
- **DO NOT INSTALL SOFTWARE OR BROWSER EXTENSIONS** BEFORE YOU HAVE CONTACTED YOUR IT DEPARTYMENT FOR ADVICE.

[Phone or text message]

We would encourage you to block the number and report the suspicious [call] [text].

Thank you again for helping to keep our network, and our people, safe from these cyber threats.

Best regards,

[Name]

[Position]

Appendix II - Letter B

Dear [Name],

We are currently received a number of reports regarding a suspicious [email] [phone call] [text message] pretending to be from [Name].

If you have received similar communications, please notify the WFN Office on reportphishing@wfneurology.org so we can monitor the situation and if necessary issue a wider alert to all WFN Trustees and people who we work with.

Thank you again for helping to keep our network, and our people, safe from these cyber threats.

Best regards,

[Name]

[Position]

Appendix III - Letter C

Dear [Name],

Thank you for alerting WFN to the scam [email] [phone call] [text message] you have received. We are currently monitoring reports in case this is a concerted campaign targeting WFN staff, trustees and people working with WFN across our many activities.

If you have already responded to the suspicious message before realising, or have clicked on any links, opened attachments, or are a victim of actual fraud, we would advise that you take the following steps:

- If you’ve been tricked into providing your banking details, contact your bank and let them know.
- If you have paid money, gather all documentation regarding the transaction and emails/invoices received and report the incident as soon as possible to your local police. IMMEDIATELY alert your bank or credit card company to the fraudulent transaction. They should immediately try to re-call the funds.
- If you think your account has already been hacked (you may have received messages sent from your account that you don't recognise, or you may have been locked out of your account), refer to the UK National Cyber Security Centre (NCSC) guidance[4] on recovering a hacked account.
- If you received the message on a work laptop, computer, or phone, contact your IT department and let them know.
- If you opened a link on your computer, or followed instructions to install software, open your antivirus software if you have it, and run a full scan. Allow your antivirus software to clean up any problems it finds.
- If you've given out your password, you should change the passwords on any of your accounts that use the same password.
- If you've lost money, tell your bank, or credit card company, and report it as a crime.

If you think you've been the victim of a scam, report it to Action Fraud[5] (in the UK) or equivalent government agency or regulatory body in your country if one exists.

Thank you again for helping to keep our network, and our people, safe from these cyber threats.

If you have any questions, please contact us at reportphishing@wfneurology.org.

Regards,

[NAME]

[4] UK National Cyber Security Centre: https://www.ncsc.gov.uk/section/active-cyber-defence/guidance-resources

[5] https://www.actionfraud.police.uk