World Health Organization

Memorandum

TO: Internal staff members and stakeholders

FROM: [REDACTED], WHO Chief Information Security Officer

DATE: June 21, 2021

SUBJECT: Recent Cyber Attacks

The World Health Organization and other institutions have been increasingly facing attempted cyber attacks from a variety of hackers and cybercriminals . Perpetrators are aware that both people and companies are overwhelmed by the COVID-19 pandemic and have resorted to targeting the medical industry when society needs it the most. When these types of attacks are carried out, whether unsuccessful or otherwise, the strain on resources detracts from focusing on the pandemic and the health and safety of the public. This can lead to a prolonged pandemic and an unnecessary loss of human life.

Cybercriminals have been targeting top officials from within the organization and attempting to phish passwords and other sensitive material. A cybercrime group known as 'DarkHotel' recently managed to construct a fake WHO website that mimics our own internal email system, allowing them to send spoofed emails and WhatsApp messages to WHO staff and members of the public. These messages often contain malicious links that steal login credentials and other information from users if clicked on. For additional security at the technical level, we have begun implementing Domain-based Message Authentication, Reporting, & Conformance (DMARC) and it will be fully automated within the next two weeks; DMARC is projected to reduce impersonation attempts by almost 75%.

Human beings can be either the weakest or the strongest part of cybersecurity, depending on how prepared and perceptive they are. Moving forward, we must all increase our diligence to bolster our security at the social level in order to thwart the attempts of these ruthless cyberattackers. Here are some policies to follow to prevent future issues: Ensure that recipients and senders you communicate with are legitimate and authenticated, never give out your login credentials, don't open attachments from unrecognized sources, always check to make sure websites you visit are secured via HTTPS, don't give out bank info, and don't feel rushed or pressured to respond to requests for personal information. By following these steps, we can reduce cyber attacks and continue building a fairer, healthier, and safer world for everybody to prosper in.