Solidarity Playbook

Regaining access to a social media account

International Civil Society Centre

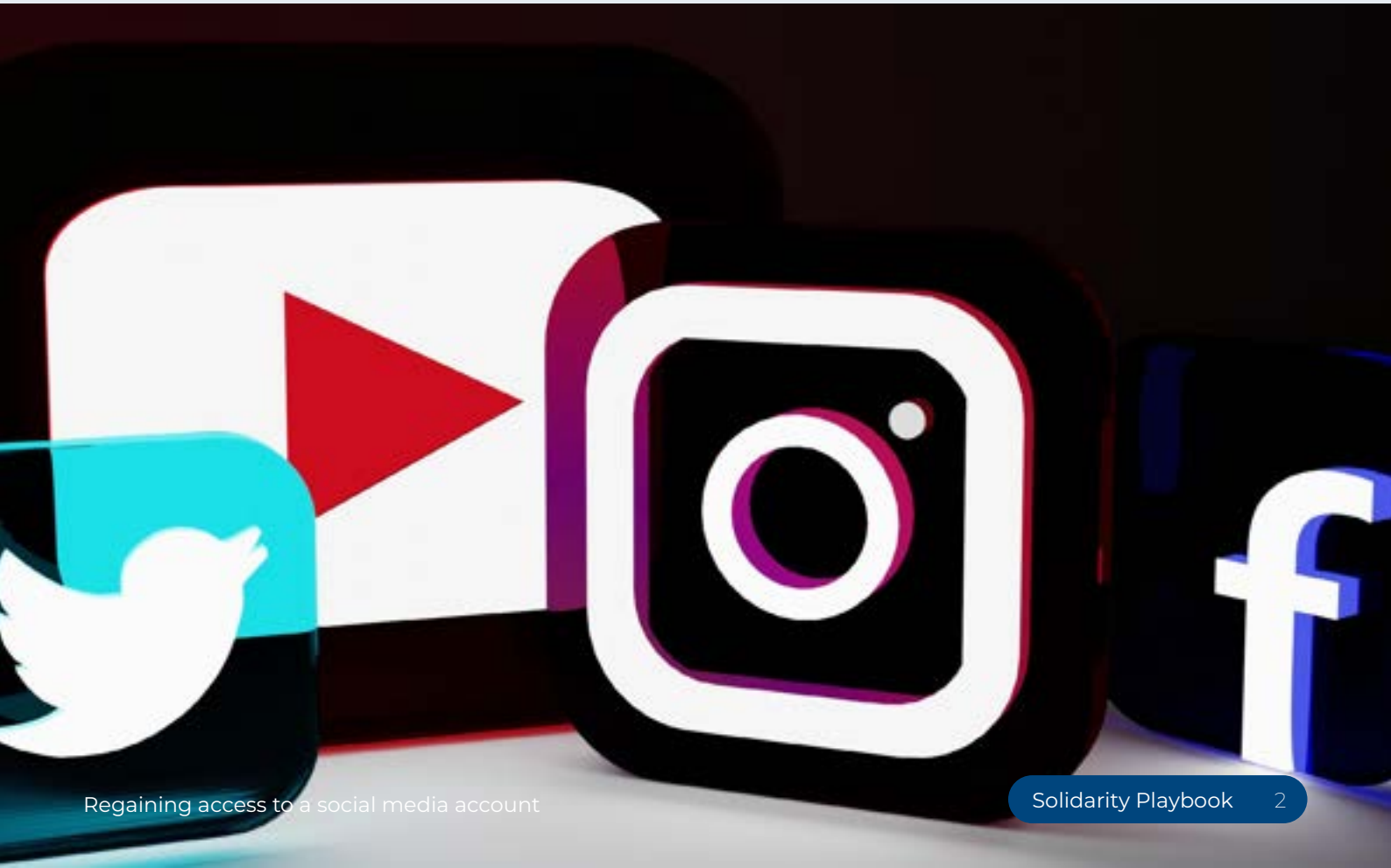
CyberPeace Institute

solidarityaction.network

1. Overview

The **Union for International Cancer Control (UICC)** is a non-governmental organisation which unites and supports the cancer community to reduce the global cancer burden, promote greater equity, and ensure that cancer control continues to be a priority in the world health and development agenda. UICC is a membership organisation that brings together 1,200 organisations around the world and works at the regional and global levels to support its members. The team includes a staff of approximately 40 employees, most of whom work from an office in Geneva.

UICC faced a social media phishing attack in the summer of 2021, which resulted in the hijacking of the organisation's World Cancer Day Instagram account. At the time, the account had 20,000 followers, and the team was concerned about this community for an important cause – which they had grown over several years – being extorted by malicious actors. Although the team had received phishing emails in the past, the sophisticated nature of this attack – which closely mirrored a real email from Instagram – made it difficult to recognise as a phishing attack.



Regaining access to a social media account

2. What happened?

The **Union for International Cancer Control (UICC)** manages the social media accounts for World Cancer Day, which is held annually on 4 February. In the summer of 2021, the UICC employee who managed the World Cancer Day Instagram account received an email from what they believed was Instagram, asking them to establish that they had the rights to use an image. They would occasionally get these kinds of queries, and the email visually looked very much like it was from Instagram. Thus, the manager of the Instagram account responded with the information requested, which included the login details for the account.

The **spear phishing email** was received on Friday. As nothing happened immediately, it seemed legitimate. But two days later, hackers contacted the employee managing the Instagram account via WhatsApp, as they had the phone number connected to the account, which was the social media manager's work phone. **The hackers demanded 10,000 euros to restore the account to UICC**. When they received the WhatsApp message, UICC staff realised that the Instagram account had been hacked and they could not access it.

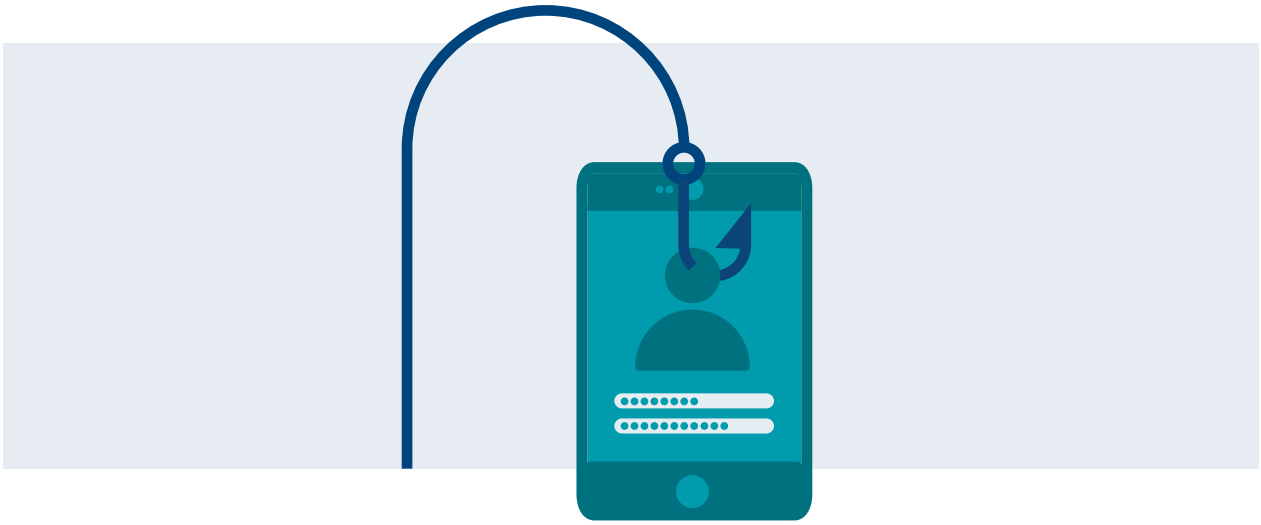
PHISHING ATTACK

A phishing attack is a common cyber threat that consists of a fraudulent communication posing as a reputable source. It aims to trick the recipient into providing sensitive data or installing malware. Phishing attacks are not only increasing in number but posing more sophisticated threats. For example, **spear phishing** is a targeted phishing attack that exploits real information about the victim to make the source of the attack seem credible.

Solidarity Action Network (2022): ***Navigating cybersecurity: Guidance for (I)CSO professionals***

Understandably, UICC was concerned about the risks of another entity controlling the Instagram account. UICC has established a reputation as a leading global health organisation and is trusted by its members. This reputation also applied to the awareness raising day, World Cancer Day. The World Cancer Day Instagram account was established in 2014, and UICC had built a significant following of almost 20,000 people on this account. **UICC feared that the hackers might capitalise on the goodwill of World Cancer Day supporters who followed the Instagram account by posing as UICC or World Cancer Day to approach them for "donations"**.

On an individual level, the employees involved in the cybersecurity incident were worried and alarmed that it had happened and angry at having been tricked. The staff member managing the social media accounts was very experienced, so there was a sense within the communications team that the **attack could have happened to anyone because the phishing email looked so genuine**. Senior management was supportive, though they had not dealt with a cybersecurity incident like this before, nor were they fully prepared to do so. As one senior manager recounted, *"You hear all these horrible things that happen through cyberattacks."* In the midst of the phishing attack, the team was thinking of worst-case scenarios (which, fortunately, did not happen).



3. Response

As soon as UICC realised that the Instagram account had been hacked and they could not access it, the communications team contacted Instagram to try to regain control of the account. However, to restore the account, they needed to verify it using the phone number connected to the account, which had been changed by the hackers. As all the information related to the account had been taken and changed, it seemed impossible for UICC to regain access. The issue was neither technical nor related to intellectual property concerns; therefore, UICC staff were redirected from one webpage to the next in Instagram's help centre. They found it frustrating that they couldn't reach a human to explain what had happened. One staff member described communicating with Instagram to reclaim the account: *"It's like a wall, you don't know how to navigate your way through it. If you can't give the missing piece of the puzzle, you can't find a way through it."*

UICC contacted their IT provider for support but were told that social media was beyond their scope. Staff reached out to the CyberPeace Institute as well, which supports organisations as they prepare for and recover from cyberattacks. The CyberPeace Institute does not offer incident response, but they did share technical and strategic recommendations with UICC. Unfortunately, in this case, the only applicable advice was to follow the process recommended by Instagram to retrieve the hacked account.

RECOMMENDATIONS TO RETRIEVE A HACKED SOCIAL MEDIA ACCOUNT

At the time of the incident, the CyberPeace Institute made the following recommendations to UICC:

Technical recommendations

- Change the passwords of every online account (particularly social media accounts) related to the email address involved in the Instagram hack.
- Implement multi-factor authentication (MFA) on all accounts and platforms if not already activated.
- Be alert to any other suspicious activity and logins related to the Instagram account and other online accounts.
- If possible, share a copy of the phishing email with experts so they can run a forensic analysis to find out more information about the attack and the cyber criminals behind it.

Strategic recommendations

- Communicate about the incident with partners and community. To protect the organisation's reputation, they recommended that UICC communicate that they had recuperated the Instagram account and no personal data had been leaked.
- Be transparent about the incident and verify with the community if unreasonable demands were made (such as fundraising via Instagram or similar actions that the cyber criminals could have taken).

Internally, the incident was immediately communicated to senior management and then staff, explaining what had happened and how it had happened and warning them to be cautious. At the time, the communications team were unsure if the phishing attack was a one-off or more would follow, so they wanted staff to be wary.

Fearing that the hackers could control the account and potentially cause harm, UICC wanted to **rapidly communicate the incident to their members** and the cancer community. First, they explained the incident on their website almost immediately after staff were informed. This information was then shared on UICC social media channels. The website post text was distributed in the organisation's regular newsletter a few days later. The communications team decided to share what had happened with their membership and the wider cancer community to prevent any further harm.

The communication was crafted to inform their target audience about **what they needed to know** – to be aware that the account was hijacked and to be wary of any approaches originating from the Instagram account. However, intricate details of the incident were not shared. Importantly, **blame was not placed on the individual who had clicked the link**, as there was a sense that any of the other six people on the communications team would also have been susceptible to this kind of phishing attack.

After communicating about the attack, UICC received some messages of solidarity. Through this communication, they actually found a solution and received the help they needed to reclaim the account. A friend of UICC who saw the post reached out to the team and helped them contact a person who worked at Meta, Instagram's parent company. That person was then able to help them retrieve the account. UICC had to answer questions about the history and use of the Instagram account to prove that they were the true account owners. In just a few days, the account was back under their control.

Ultimately, it was by chance and through personal connections, rather than formal channels, that the team were able to regain control of the World Cancer Day Instagram account. They communicated this news on their website 13 days after the initial post about the account being hijacked. If the team had not been able to recover the World Cancer Day account, they likely would have had to set up a new account. The team was also exploring legal action, but in the end, they did not need to take such action because the issue was resolved through the personal connection to a Meta employee.

World Cancer Day Instagram account has been hijacked

Convening Members Partners Networks

3 September 2021

At the end of August, the World Cancer Day Instagram account managed by UICC was the target of a cyberattack and has been stolen, or "phished". The account is now compromised.

UICC is the lead organiser of World Cancer Day, which has become one of the most important health awareness days of the year and is celebrated on 4th February.

Unfortunately, the World Cancer Day Instagram account fell victim to a cyberattack at the end of August and was hijacked. The account can no longer be accessed. UICC is taking legal action.

Please be careful if you are being approached via the World Cancer Day Instagram account in any way, as it is no longer in safe hands. These phishing attacks are becoming increasingly sophisticated and illegitimate emails are unfortunately harder to spot.

UICC strongly condemns the attack. Several attempts to reach out to Instagram for assistance have met with either no response or the claim that our complaint cannot be received as it is considered neither an intellectual property violation nor an infringement of UICC's legal rights.

No doubt **World Cancer Day supporters will prove their resilience and unfaltering support and soon rally again on Instagram once a new account has been created** to fight for this important cause.

In the meantime, UICC is working on an exciting new campaign for 4th February 2022 and looks forward to sharing it soon.

Tags: World Cancer Day WCD 2022 Instagram Phishing

Screenshot from UICC website, which shows how they communicated the incident to the community on 3 September 2021. They followed up with another post on 16 September to communicate that the account had been retrieved.

4. Outcome & impact

Ultimately, the phishing attack did not affect the campaign for World Cancer Day. At the time of the attack, about six months before the annual World Cancer Day on 4 February, the account was quiet (typically, it becomes more active in the months leading up to the awareness day).

Following the incident, UICC staff were more alert. Although they were already aware of phishing attempts and knew not to click strange links in emails, the deceptive nature of the incident – **how *real* the phishing email looked** – meant that staff were double- and triple-checking anything that appeared unusual. This alertness was also transferred to new staff during handovers of job responsibilities. For example, the outgoing social media manager briefed the new social media manager about the Instagram phishing attack, including the level of sophistication.

In the aftermath of the attack, UICC staff underwent training, and the communications team made sure that the social media accounts were set up with the strictest possible protections. They received a cybersecurity training from the CyberPeace Institute on other phishing and cyberattack tactics that the team were not aware of. For example, they learned about a strategy in which cyber criminals would leave a USB stick in offices titled "staff salaries," so that curious staff members would then insert them into their work computer to read, giving cyber criminals access to the organisation's computer network by downloading malware. By learning about the different tactics used to initiate cyberattacks, the team was more alert to them. UICC management felt that this alertness could help the staff minimise human error as much as possible.

MALWARE

Malware is a malicious software. These are pieces of code designed to damage, destroy, or subvert computer systems. Malware includes viruses that can replicate and stop systems from working; ransomware, which blocks systems until a ransom is paid; and spyware, which is hidden on the target system to spy on the device users.

CyberPeace Institute (2022): ***Glossary of cyber terms***

The UICC team made several changes following the incident. The team added multiple layers of verification and authentication on their social media accounts, so that one person can no longer change the credentials.

Prior to the incident, cybersecurity was a bit of an abstract concept: there was a general idea that UICC should be secure. In the aftermath of the incident, this concept became more concrete, and UICC became more aware of actions they could take to protect the organisation. In particular, the incident created greater awareness of cybersecurity among senior members of the organisation, which has **translated to new organisational processes and tools**. For instance, cyber risks are now included in the organisation's risk matrix, which had previously only covered technical issues, such as if the internet or phone lines stopped working. The new risk matrix includes specific cybersecurity threats and the reputational risk of cybersecurity incidents.

While the Instagram phishing attack was a one-off incident, UICC has long received phishing attempts on a monthly basis. The phishing emails have become more sophisticated over time (for example, they used to have typos and no longer do), but staff members now know what to look for in the email address to identify a phishing email. These days, as soon as a phishing attempt is received, a screenshot of the email is shared to notify all team members. UICC has found that new staff members are particularly targeted by phishing attacks. There is a pattern of a phishing email which appears to originate from the CEO, asking new staff members to run errands. This has become a running joke on the team, and all new staff members are told that if they receive an email asking them to buy socks or iTunes cards for the CEO (as the phishing emails often request), they should not respond!

CYBERCRIMINALS OFTEN TARGET NEW STAFF

UICC management has noticed that new staff members are particularly targeted by phishing attacks, which is common across many organisations. Cyber criminals pay attention to job updates that individuals post on social media (particularly LinkedIn) and then craft phishing emails which target these individuals. Further, if cyber criminals are targeting a specific organisation, they tend to keep an eye on any changes to the organisation's website (such as posts introducing new staff members). These reconnaissance methods have become common among cyber criminals, who will use them to try to enter the organisation through the new staff member.

5. Organisational learnings

CHALLENGES

Account retrieval

It was not easy for the organisation to regain access to the Instagram account. They found that the social media help desks sent them in circles, and it was only through a personal intervention that they were able to make their situation known and receive the help they needed from Meta (the parent company of Instagram).

First-time response

For staff in senior management, this was the first time they had faced such an incident, which meant they were dealing with something that they didn't know about and weren't sure what would happen. This lack of experience created some uncertainty in how to respond.

Resource constraints

As a small organisation, another challenge UICC faced was the limited resources and knowledge available for cybersecurity. They have limited resources to invest in security and a small IT budget. As is true of many organisations, UICC's focus is on the work and impact they are trying to achieve, which de-prioritises and under-resources operations.

Which team is responsible?

There was also a question of where the responsibility for cybersecurity falls, especially when an incident happens outside the realm of the IT team. Cybersecurity is usually the responsibility of IT, and if the attack had been on the organisation's email system, IT would have been responsible for responding. However, this incident took place on social media, which was managed by the communications team, who traditionally have less experience in cybersecurity than an IT team.

LESSONS LEARNED

Use multi-factor authentication

While there are no fail-safe measures in cybersecurity, multi-factor authentication (MFA) would have added an extra layer of security to the Instagram account and made it more challenging for cyber attackers to take over the account. In the aftermath of the incident, UICC implemented two-factor authentication. As a result, staff must now take a first step of entering a username and password on one device and a second step of authenticating their login using a code received on their smartphone to log into accounts.

Develop a Disaster Recovery Plan

After experiencing the first cyberattack which successfully penetrated their system, UICC management better understood how cybersecurity incidents happen. They also learned how they could better prepare and respond to an incident by having a crisis plan or Disaster Recovery Plan in place. While UICC developed their crisis plan by deciding what to do at each stage, there are also templates available, which organisations can use as a basis for their own plan.

DISASTER RECOVERY PLAN

A Disaster Recovery Plan (DRP) is a document that allows organisations to quickly resume operations or continue to operate during crisis such as a power outage, natural disaster, or **cyberattack**. The plan contains detailed, step-by-step instructions on how to respond, as well as strategies to minimise the effects of a disaster. The aim of the plan is to decrease the recovery time needed and thus limit the negative impacts to the organisation that can result from significant disruptions (such as disruption of services, lost funding, and brand damage). Organisations should include cyberattacks in their DRPs.

Kyndryl (2022): ***Disaster recovery plans explained***

Examples of a DRP template can be found on the **Disaster Recovery Plan Template** and **IBM** websites.

Seek help

The help of an organisation like the CyberPeace Institute was invaluable to UICC in mitigating risks during the incident and training staff and supporting the organisation to further strengthen their cybersecurity after the incident.

Use plain language

The UICC staff involved in the incident were not IT staff. Therefore, they appreciated that the organisation they sought help from spoke about cybersecurity in a language they could understand. Technical terminology can be intimidating for staff working outside of IT, and senior managers at UICC felt comfortable asking questions of the CyberPeace Institute staff.

Promote a no-blame culture

The Instagram phishing attack prompted some staff to appreciate the culture of the organisation; namely, the importance of not blaming, promoting openness, and providing safe channels for staff to report any incidents and feel comfortable doing so.

Discover more case studies
solidarityaction.network/cybersecurity

Regaining access to a social media account

Solidarity Playbook

Regaining access to a social media account

Sacha Robehmed and Nonso Jideofor

March 2023

International Civil Society Centre

CyberPeace Institute

In partnership with

Sweden Sverige

FORD FOUNDATION