

Chapter 7

Digital Afterlives: Cyber Vulnerability and Social Belonging

Adrija Nath, Independent researcher, Jadavpur University

Abstract

In contemporary digital societies, cybersecurity is generally grounded as a technical problem, so much so that breaches are measured in financial losses, identity theft is reduced to credit score damage, and phishing is treated as a failure of awareness or digital literacy. Yet for those who experience hacking, impersonation, data breaches, or sudden deplatforming, the entire experience does not end when passwords are reset or accounts are restored. Instead, it initiates what this paper calls as a *digital afterlife* which is a chronic socio-psychological condition in which identity, their sense of belonging, and trust are reshaped by conditions of cyber vulnerability. This study moves the focus away from technical fixes to people's real-life experiences. It argues that cyber victimisation is not just about financial loss, but a deep disruption to a person's social life and sense of stability. Using in-depth interviews with people who have gone through hacking, identity theft, phishing scams, or being removed from online platforms, this study places these experiences within wider sociological ideas such as stigma, trauma, social identity, and trust in institutions. Drawing on Erving Goffman's idea of a "spoiled identity," the paper shows that many victims begin to blame themselves after such incidents. They often feel ashamed and describe themselves as careless, naïve, or lacking digital skills. These experiences show that it is not just personal embarrassment at play, but also a broader cultural belief that online safety is primarily an individual's responsibility. As a result, being a victim of cybercrime becomes a stigmatised condition, something people often keep hidden, rarely speak about openly, and one that is closely tied to judgments about a person's competence in the digital age.

The paper also tries to understand cyber victimisation as a kind of identity trauma. Unlike ordinary property crimes, digital breaches unsettle the line between who a person is and how they appear online. When someone's email is hacked, their social media is impersonated, or their account is suspended without any explanation. Their digital self, which in today's world is very central to work, relationships, and public life, becomes fragile and exposed. Participants describe feeling detached from themselves and exposed, almost like as if they have lost control over their own story and identity. Especially in cases of suspension of profiles, people describe a feeling of being erased from public life. Losing access to a platform is seen as a social exclusion from spaces where their friendships, work opportunities, and political voice are rooted.

The study also looks into how cyber vulnerability changes people's trust in institutions. Many victims describe a second layer of harm when they face unclear and unsupportive customer service systems, and a sense of bureaucratic indifference. Banks, online platforms, and government agencies often come across as distant, impersonal, and hard to deal with. As a result, people's trust in these institutions is often shaken. The effects of a breach therefore go beyond personal anxiety,

leading to a wider sense of doubt and mistrust toward the systems and institutions that govern digital life.

The study also reflects that the long-term effects of cyber incidents are not experienced equally. People with limited digital skills, insecure jobs and thus people who are marginalised socially often face stronger stigma and take much longer to recover. For instance, the freelance workers and content creators, when removed from a platform means endangering their livelihood. For women and people from marginalised gender identities, hacking and impersonation often bring extra reputational damage and moral scrutiny. Cyber vulnerability therefore works through the already existing social inequalities, making already precarious lives more unstable. Using ideas about social identity and trust in institutions, the paper argues that digital harm is deeply social and relational. By focusing on people's life experiences, the study questions mainstream cybersecurity approaches that mainly gives more importance to prevention and financial damage, while overlooking the difficult social recovery individuals go through after a digital violation. In terms of method, the study uses narrative analysis to follow how people tell the story of a cyber incident over time, from the initial shock and confusion to the longer-term ways they cope, with it. The digital aftermath is marked by a sense of tension, people still have to rely on digital systems in everyday life, yet they trust them much less than before. In the end, the paper argues that as more of our social, economic, and civic lives move onto digital platforms, cyber vulnerability should be understood as a serious form of social harm, not just a technical risk.

Keywords: *Cyber Vulnerability, Cyber Victimization, Extra Reputational Damage and Moral Scrutiny.*

Introduction

Digital technologies now shape much of everyday social life. Emails structure work routines in offices and institutions. Messaging platforms sustain friendships and maintain contact across distance. Social media profiles often function as public markers of identity where individuals present themselves to others. For many people, the internet is therefore not a separate space that exists outside social life. It has become one of the main arenas where relationships are maintained, reputations are built, and opportunities emerge. In this sense, digital presence is closely tied to how individuals are seen and recognised by others. Despite the growing importance of digital spaces in everyday life, discussions around cybersecurity are still framed largely as technical matters. When incidents such as hacking, phishing scams, identity theft, deplatforming are discussed, the focus usually falls on data protection, financial damage, or the need for better digital awareness. Institutional advice often centres on practical precautions such as creating stronger passwords or being more careful while using online platforms. While these measures are important, they also shape how cyber incidents are understood. They come to appear as problems that can be fixed once accounts are recovered or financial losses are managed, leaving little room to consider how such experiences might affect people beyond the immediate moment of the breach.

Yet these ways of thinking about cyber incidents leave out an important part of the story: how such events are actually experienced by the people who go through them. For someone whose account has been hacked or whose profile has suddenly been taken down, the experience rarely ends when

the technical issue is fixed. Many people continue to feel uneasy about their digital presence for some time afterwards. Some speak of embarrassment, especially when others become aware of what happened. Others describe a sense of exposure, as if something personal had been briefly taken out of their control. It is also common for people to begin questioning their own abilities with digital systems, wondering whether they missed some warning sign or made a mistake along the way. For a while after the incident, even routine actions online can feel slightly different. Activities that were once automatic may now be approached with caution.

This chapter approaches cyber incidents from this experiential perspective. Instead of looking at the technical side of hacking or data breaches, the focus here is on how individuals themselves understand and recount what happened to them. What matters is not only the incident, but what follows it. How do people make sense of such moments? How do they respond to the sudden awareness of vulnerability? And how does the experience slowly reshape the way they relate to the digital systems that are part of their everyday lives?

To describe this prolonged aftermath, the chapter introduces the idea of a *digital afterlife*. The phrase refers to the state in which people continue to live with the effects of a cyber breach even after the immediate disruption seems to have been resolved. When someone's account is hacked, their identity is impersonated, or they fall prey to cybercrimes, the event often leaves behind traces that linger for some time. People begin to see their digital identity differently. Their trust in the systems that organise online life may also change.

The chapter explores three central questions. First, how do individuals narrate their experiences of cyber victimisation? Second, in what ways do such incidents influence their sense of identity and belonging within digital spaces? Third, how do these experiences affect trust in institutions such as banks, online platforms, and other systems that organise digital life?

This chapter combines primary and secondary sources to explore how people experience cyber harm in everyday life. The primary data comes from qualitative interviews with individuals who had faced incidents such as hacked accounts, impersonation, cyber bullying or loss of access to digital platforms. These conversations focused on how participants understood and coped with these experiences in their daily lives. Alongside this, the chapter draws on existing academic literature on digital identity, trust, and inequality. Bringing together personal accounts and scholarly work helped situate these experiences within the framework of social realities of life in a growing digital world.

The digital self and networked identity

Digital technologies have slowly become part of how people show themselves to others and stay connected in everyday life. Over time, these spaces begin to hold traces of everyday interactions such as messages, photographs, exchanges, payments, and memories. Because of this, digital accounts rarely feel separate from the individual who uses them. They become one of the ways through which people are recognised and remembered by others. Our digital presence today therefore, is much more than just a technical profile attached to a platform. It has become a part of how individuals see themselves and how they are seen by others.

Long before the rise of digital platforms, scholars such as *Erving Goffman*¹⁵³ suggested that everyday life involves a constant process of presenting oneself to others. People adjust how they speak, behave, and appear depending on the situation and the audience they face. A classroom, a workplace, or a gathering with friends each call for slightly different forms of self-presentation. Digital platforms extend this process into new settings. A profile page, a carefully chosen photograph, or a short biography now becomes part of how individuals introduce themselves to wider audiences. Even seemingly small choices like what to share and what to hide can shape how others perceive a person online. At the same time, these digital environments differ from earlier social settings as well. Interactions that once disappeared after the moment passed, now leave behind records that may remain visible for years. Messages, photographs, documents and posts accumulate over time, forming a kind of archive of a person's digital presence. This awareness often influences how people manage their online behaviour, encouraging a more careful form of self-presentation.

The growing importance of digital networks has also changed the spaces through which relationships are maintained. *Manuel Castell*¹⁵⁴ describes contemporary societies as being increasingly organised through networks of information and communication technologies. Work relationships, friendships, public conversations, debates, shopping, transactions frequently unfold within these digital networks. Participation in such spaces is often necessary for staying relevant and connected with the world around us.

*Anthony Giddens*¹⁵⁵ too has offered a useful way of thinking about these developments through his idea of the “reflexive projection of the self.” According to Giddens, individuals continuously reflect upon and shape their own life stories as they move through different experiences. Identity develops gradually through the choices people make, and the narratives they construct about themselves. Digital platforms have become one of the places now, where this process unfolds.

As a result, the boundary between online and offline life often becomes difficult to draw clearly.

Several participants in this study have described how closely their digital presence had become tied to their sense of everyday stability. One respondent, a freelance photographer in her late twenties, explained that most of her professional communication took place through a single email account and an online portfolio linked to social media. When she temporarily lost access to the account following a hacking attempt, she described the experience as deeply unsettling.

“It wasn’t only about the account,” she reflected during the interview. “For a few days it felt like I had disappeared from the place where my work and contacts actually exist.”

¹⁵³ Erving Goffman, *The Presentation of Self in Everyday Life* (Penguin Books 1959).

¹⁵⁴ Manuel Castells, *The Rise of the Network Society* (2nd edn, Wiley-Blackwell 2010)

¹⁵⁵ Anthony Giddens, *Modernity and Self-Identity: Self and Society in the Late Modern Age* (Polity Press 1991) ¹³⁷ Sherry Turkle, *Life on the Screen: Identity in the Age of the Internet* (Simon & Schuster 1995).

Sherry Turkle's¹³⁷ work on digital life offers a helpful way of thinking about how these spaces gradually become part of how people understand themselves. In her writings on life with computers and the internet, Turkle suggests that digital environments create new spaces where individuals can express and sometimes even experiment with different parts of their identity. Through conversations, posts, photographs, or messages, people begin to share fragments of their everyday lives online. Over time, these fragments form a visible presence through which others come to know them. Turkle points out that this process is not only about communication across distance. Online spaces also allow individuals to find communities that share similar interests, experiences, or concerns. Someone who feels unheard or unnoticed in one setting may find recognition in another digital space. And any disruption to this side of our lives gives meaning to what we can call a *digital afterlife* which is like a lingering condition that can follow a cyber incident long after the immediate problem appears to have been resolved.

Experiences of cyber victimisation are often accompanied by feelings that go beyond the immediate shock of the incident. Alongside confusion or anxiety, many individuals also describe a quieter emotion that surfaces soon afterwards that is embarrassment. Even when people recognise that they have been targeted by sophisticated scams or hacking attempts, they frequently speak as though the event reflects some personal mistake on their part. In conversations about cyber incidents, it is not uncommon to hear individuals describe themselves as having been “*careless*,” “*naïve*,” and “*not careful enough*.” The language people use to recount these experiences often carries a tone of self-blame.

One way to understand this reaction is through Goffman's¹⁵⁶ discussion of stigma. He described stigma as a situation in which certain experiences or attributes come to be seen as discrediting within a particular social setting. When this happens, individuals may begin to feel that something about them has been judged negatively by others. They may try to conceal the experience or even internalise the judgement themselves. In such situations, the issue is not simply the event that took place, but the social meaning that is attached to it.

Cyber victimisation can easily take on this kind of meaning. In an environment where digital competence is increasingly taken for granted, people are often expected to know how to protect themselves online. Advice about cybersecurity regularly emphasises individual vigilance for instance recognising suspicious emails, avoiding unknown links, managing passwords carefully and report suspicious calls. While such guidance is important, it also creates a subtle expectation that responsible users should be able to avoid these risks. When something does go wrong, the incident can therefore feel less like a random misfortune and more like a personal lapse.

One participant in this study, a postgraduate student, recalled how uncomfortable she felt telling her friends that her email account had been compromised after she responded to a phishing message. Although she later realised that the email had been carefully designed to appear legitimate, her first reaction was embarrassment. During the interview she explained:

¹⁵⁶ Erving Goffman, *Stigma: Notes on the Management of Spoiled Identity* (Prentice-Hall 1963).

“I kept thinking I should have noticed something was wrong. It made me feel like I had been careless, even though the message looked very real at the time.”

Another participant described a similar hesitation when discussing a social media account that had been temporarily taken over by someone impersonating him. Even after the account was recovered, he admitted that he had not told many people about the incident.

“It felt strange to talk about,” he said. “You start wondering what others will think. Maybe they will assume you weren’t paying attention or you are a technological handicap”

These reactions they show how cyber incidents can quickly become framed as individual failures. Instead of viewing themselves simply as victims of a crime, individuals may begin to interpret the event as evidence that they were not sufficiently cautious or knowledgeable. In Goffman’s terms, the experience can threaten a person’s sense of competence and produce what he described as a *“spoiled identity.”* The individual may feel that something about their social image has been damaged, even if the incident itself was beyond their control. This sense of embarrassment often leads people to limit how openly they speak about what happened. Some respondents mentioned that they only told a small circle of close friends, while others avoided discussing the incident altogether. The reluctance to share these experiences is shaped partly by the fear of judgement.

One respondent, a young professional working in a technology-related field, spoke about how difficult it felt to admit that she had been the target of a phishing attempt that briefly compromised her account.

“Because I work in a field where everyone is supposed to be digitally aware, it felt almost worse,” she explained. “I kept thinking that people would expect me to know better.”

Her reaction reveals how expectations surrounding digital competence can heighten this sense of personal failure when something goes wrong.

News reports and public campaigns frequently emphasise caution and awareness, sometimes implying that those who fall victim to scams may have ignored obvious warning signs. Although such messages aim to encourage safer online practices, they can unintentionally reinforce the belief that victims are responsible for their own misfortune. This cultural expectation is what places us in a difficult position making it an intersectional issue.

Identity Trauma and the Fragility of the Digital Self

When a cyber incident takes place, the first concern is often practical that is recovering the account securely and preventing further damage. Yet for many individuals, the experience does not end here. Over time, the incident can begin to affect how people think about their own digital presence and their sense of control over it. Digital accounts often hold much more than access to a platform and because of this, losing control over such an account can feel upsetting in ways that extend beyond technical control.

Anthony Giddens¹⁵⁷ understands this reaction through the idea of ontological security. He uses this term to describe the sense of stability that individuals rely upon to move through everyday life

with confidence. People develop routines and expectations that allow them to trust that the world around them will remain reasonably predictable. This sense of continuity is not always something individuals consciously think about; rather, it quietly supports the feeling that everyday life makes sense and remains under some degree of control. Digital systems have gradually become part of these everyday routines. Checking email, responding to messages, or logging into accounts or making online purchases or payments often happens almost automatically. Over time, these activities create a sense of familiarity with the digital environments people rely upon. Whenever there is a breach in this environment without warning, that sense of familiarity can be deranged. The experience can make individuals aware that something they once trusted can suddenly become uncertain.

Participants in this study when asked about this described this moment of disruption quite vividly. One respondent recalled discovering that someone had briefly gained access to her social media account and had begun sending messages to people in her contact list. Although the situation was resolved within a few hours, she described the experience as –

“For those few hours, I kept thinking that someone else was speaking as me. It felt strange to imagine that people might read those messages and think they came from me.”

Such experiences point to the fragile boundary between a person and the digital representations through which others encounter them. When someone impersonates an account or gains access to a personal profile, that boundary becomes dimmed. The account continues to exist in public view, but the individual behind it may no longer have control over what appears there. In that moment, a digital identity can begin to feel detached from the person it represents.

Kai Erikson's¹⁵⁸ work on trauma provides another way to think about this sense of disruption. Erikson described trauma not simply as a response to physical harm but as an experience that shaken a person's sense of continuity and belonging. Trauma, creates a feeling that the familiar order of things has been disturbed. While cyber incidents differ greatly from the kinds of disasters Erikson originally wrote about, the underlying idea of disruption can still be useful. For some individuals, losing control over their digital identity produces a moment of disorientation. Accounts that once felt like stable extensions of their everyday life begin to appear fragile and uncertain.

Another participant described this experience after his professional email account was briefly compromised. Although no significant damage occurred, he remembered feeling uneasy even after the account was secured again. *“I kept thinking about how much of my work life is in that account,”* he said.

¹⁵⁷ Anthony Giddens, *The Consequences of Modernity* (Polity Press 1990).

¹⁵⁸ Kai Erikson, *Everything in Its Path: Destruction of Community in the Buffalo Creek Flood* (Simon & Schuster 1976).

“If someone can step into that space, even for a short time, it makes you realise how exposed things actually are.”

Account suspension can produce a different but related feeling. In these cases, individuals do not lose control because someone else takes over their identity. Instead, they find themselves suddenly removed from a digital space where they previously had an active presence. One respondent explained that losing access to a platform where she had spent years sharing photographs and writings made her feel as though a small part of her social life had been abruptly cut off.

“It was strange,” she reflected.

“It wasn’t just about posting pictures. It felt like a place where my life had been unfolding had suddenly closed its doors.”

These reactions they show how digital identities today, have become intertwined with everyday social interactions. Some participants also described a lingering awareness of vulnerability after the incident had passed. Even once accounts were recovered or secured, the earlier sense of certainty rarely returned in the same form. Routine activities such as logging in or sharing information began to carry a new layer of caution.

Institutional Trust and Bureaucratic Indifference

When people become victims of cyber incidents, the harm rarely ends with the initial breach. The experience often extends into a quieter struggle that involves navigating institutions that are supposed to help. Banks, online platform, customer support systems, and cybercrime authorities become the next points of contact. In theory, these organisations exist to restore order and protect individuals. In practice, many victims encounter something very different. Automated messages, complicated procedures, delays in follow ups and distant forms of communication t feel impersonal and slow. What begins as a technical problem quickly becomes a crisis of trust.

Trust plays a central role in how modern digital environments function. Individuals believe the systems managing their online activities are reliable. The idea of trust explored by *Niklas Luhmann*¹⁵⁹ helps explain this dynamic. Luhmann suggested that trust reduces complexity in everyday life. In a world filled with uncertainty, people rely on trusted institutions and systems so that they do not have to question every interaction or decision. Without this reliance, ordinary activities would become overwhelming. Digital infrastructures depend heavily on this kind of trust. Most users do not fully understand the technical mechanisms behind online platforms. Instead, they assume that these systems will work as promised. The presence of passwords, verification processes, and security alerts gives the impression that protection is built into the structure of the system. If things run smoothly, this trust remains largely invisible.

Problems arise when the system fails. A hacked account, fraudulent transaction, stolen identity or cyber bullying disrupts the quiet confidence people place in these systems. Suddenly, what once

¹⁵⁹ Niklas Luhmann, *Trust and Power* (John Wiley & Sons 1979)

felt routine becomes uncertain. At this moment, victims often turn to institutions for assistance. The expectation is simple that is someone will listen, investigate, and help restore what has been lost. However, the reality is quite different.

Let us consider the experience of contacting customer support after an online account has been compromised. Many platforms rely heavily on automated systems to manage large volumes of complaints. Victims are frequently directed through layers of help pages and chatbots before they reach an actual person, if they reach one at all. While these systems are designed for efficiency, they can feel deeply frustrating for someone who is already dealing with anxiety and confusion. The language of automated responses often sounds neutral and procedural, yet to victims it can appear dismissive or indifferent. A similar experience can emerge in interactions with banks following digital financial fraud. Victims may spend hours explaining their situation, submitting documentation, and waiting for internal investigations. During this period, uncertainty lingers. The individual is left wondering whether their money will be recovered, whether the institution believes their account of events, and whether the system truly prioritises their protection. Even when banks eventually resolve the issue, the process itself can leave a lingering sense of vulnerability.

The concept of trust in modern systems developed by *Anthony Giddens*¹⁶⁰ provides a useful way to understand this experience. Giddens argued that modern societies rely on what he called “*abstract systems*” which is a large, complex networks of expertise and technology that people depend on without fully understanding how they operate. For examples, we can take financial institutions, technological infrastructures, digital platforms and online payments. People interact with these systems daily, trusting that they are managed by competent experts. Cyber incidents expose the fragile nature of this reliance.

When something goes wrong, individuals suddenly confront the distance between themselves and the systems they depend on. The result is a feeling of disconnection. Victims may feel that their personal crisis has been absorbed into an impersonal administrative process. Further, interactions with cybercrime authorities can reinforce this sense of distance. Victims often describe feeling as though their experiences have been reduced to case numbers within a system that moves slowly and communicates little.

This bureaucratic character of institutional response can be better understood through the work of Max Weber¹⁶¹. Weber described bureaucracy as a rational organisational structure designed to maximise efficiency through rules, procedures, and hierarchies. Such systems are meant to produce consistency and fairness by treating cases according to standardised guidelines rather than personal judgement.

Yet bureaucracy has a paradoxical side. While its structured procedures are meant to ensure fairness, they can also produce emotional distance. Individuals facing urgent or distressing situations may feel that the system responds too slowly or too rigidly. The rules that keep

¹⁶⁰ Anthony Giddens, *The Consequences of Modernity* (Polity Press 1990) 27–29

¹⁶¹ Max Weber, *Economy and Society: An Outline of Interpretive Sociology* (University of California Press 1978).

institutions organised can also make them appear indifferent to the personal realities behind each case. This phenomenon can be described as secondary victimisation. The initial attack may involve financial loss, identity misuse, or the invasion of personal information. The institutional response, however, can unintentionally deepen the sense of vulnerability. Victims who struggle to obtain clear answers or timely support may begin to question whether the systems they trusted are truly capable of protecting them.

Inequality and Differential Cyber Vulnerability

Cyber harm is almost never socially neutral. While digital spaces often present themselves as open and universal, the risks and consequences attached to cyber incidents are quite unevenly distributed. People's social positions, play a significant role in determining how deeply they are affected. For some individuals, a cyber incident may be frustrating but manageable. For others, it can threaten their livelihood, reputation, or sense of safety. To understanding this uneven landscape it's important to grasp the of *digital divide*. This concept is not only about who has access to the internet but also about who feels confident accessing the digital systems. Individuals with strong digital literacy often recognise warning signs such as suspicious login alerts or phishing attempts. They may also know how to recover accounts, report incidents, or secure their information quickly. But those users who are less familiar with digital technologies often struggle to interpret what has happened or how to respond.

One participant, a 52-year-old tailoring service provider who had recently begun accepting online orders, described how difficult it was to deal with a phishing scam that compromised her messaging account:

“My customers started telling me they received messages asking for advance payments. I didn't even know someone had taken control of my account. My son had to sit with me and figure out what was happening.”

Her experience reflects the uncertainty that can accompany limited digital familiarity. The breach itself was stressful, but the process of understanding the problem felt equally overwhelming. Instead of acting independently, she relied on younger family members to learn the technical aspects of account recovery.

Economic vulnerability also shapes how cyber incidents unfold. Freelancers and gig workers often depend entirely on digital platforms for visibility, payments, and client relationships. When these platforms malfunction or accounts become inaccessible, the consequences are immediate. One participant who worked as a freelance translator described how a security flag temporarily froze her payment account:

“The platform said they were reviewing my account for suspicious activity. During that time, I couldn't withdraw anything. I had already completed projects, but the money was stuck there. For two weeks I was just waiting and hoping they would clear it.”

For her, the delay was not merely inconvenient. As someone without a fixed salary, access to that payment was crucial for covering monthly expenses. The platform's automated security measures, though designed to prevent fraud, ended up magnifying the precariousness of her situation.

Gendered expectations too influence how cyber harm is experienced. Several women participants spoke about the reputational anxieties that followed digital incidents. The fear was not simply about technical loss but about how others might see them. A postgraduate student described the distress she felt after discovering that someone had circulated edited screenshots of her social media posts in a private online group:

"They changed the captions and made it look like I had written things I never said. Even after I explained it was fake, I kept worrying about who had seen it."

In her case, the harm came less from the technological act itself and more from the social consequences attached to being the secondary sex. For individuals with marginalised gender identities, cyber incidents often intersect with the already present experiences of discrimination. Digital platforms may offer opportunities for visibility and connection, yet they can also become spaces where harassment and targeted attacks occur.

One interviewee, who identifies as a transgender man and runs a small online art page, described receiving repeated attempts by strangers to access his account:

"At first I thought it was random hacking attempts. But then I realised people were also sending messages saying things like 'people like you shouldn't be online.' That's when it started feeling personal."

The experience blurred the boundary between a technical threat and social hostility. What might have been let go as routine hacking attempts in another context became a question linked to his identity.

Another participant, a young non-binary student, spoke about the vulnerability of relying on online communities for emotional support:

"Most of my support system is online. When someone reported my account and it got temporarily restricted, I felt cut off from everyone who understood me."

For them, the platform was not just a communication tool but a crucial space for belonging. Losing access, even briefly, created a sense of isolation. These real life experiences reveal how cyber vulnerability is closely tied to broader social inequalities.

Living in the Digital Afterlife

Cyber incidents are often spoken about as - something goes wrong, the account is recovered, and life continues. But as we have understood for people the experience does not end when the technical part of it is resolved. The breach leaves behind a residual thought that their digital identity can be accessed, breached, altered, impersonated, and taken away without warning. The repercussion becomes a kind of *digital afterlife*. The event itself may pass, but the feeling remains.

For many victims, the experience begins with *shock*. The first moment of discovering that something is wrong rarely feels clear or immediate. Strange notifications, unfamiliar posts or unexpected transactions create confusion. Digital accounts usually feel stable and predictable, so the idea that someone else may be inside them is difficult to process. Once the reality of the breach becomes clearer, the emotional response often shifts inward. The second stage is quite often marked by *self-blame*. Instead of focusing only on the attacker or the system failure, individuals begin questioning their own behaviour. They wonder whether they could have done things differently. Even when cyber incidents are complex and difficult to prevent, victims often feel that they should have been more careful. This quiet sense of embarrassment can make people hesitant to talk openly about what happened.

After this comes a more practical but often frustrating phase which is the *struggle to regain control*. Individuals must deal with these platforms in order to recover their accounts or secure their information. While these processes are designed to protect users, they can feel slow and impersonal. The breach itself may have taken minutes, but the effort to repair its consequences can last much longer. Even after access is restored, many people find that their relationship with digital spaces has changed. A period of *social withdrawal* often follows. This does not always mean abandoning online platforms altogether, but participation becomes more cautious. People post less or think twice before engaging online. Activities that once felt effortless begin to carry a small sense of risk.

Over time, most individuals reach a stage of *adaptation*. They develop new habits which could be having stronger passwords, additional security settings, or more careful digital routines. These adjustments help restore a degree of stability, but they don't quite bring back the original sense of trust. Instead, digital life continues with a constant awareness that things can go wrong. In such a way, cyber harm often becomes less like a temporary interruption and more like a *chronic condition*.

Conclusion

Cyber incidents are often treated as technical mishaps. Yet the experiences discussed in this chapter suggest that the damage does not stay within the realm of tech. When a digital account is compromised, what is shaken is not just a platform but the person attached to it. Digital profiles today hold fragments of our identity. When these spaces are breached, the boundary between the self and its online representation suddenly feels brittle, leaving individuals feeling exposed or oddly detached from versions of themselves circulating online. At the same time, cyber incidents quietly reshape belonging. Because friendships, work, communities, and services now exist largely on platforms, losing access even briefly can feel like being locked out of a room where social life continues without you. The result is sometimes withdrawal, with individuals becoming more cautious about what they share and how they participate online from then on. These experiences also affect trust in institutions. Cyber vulnerability also tends to mirror existing inequalities—freelancers dependent on platforms risk losing income, individuals facing social scrutiny risk reputational damage, the differential experiences that comes with belonging from different social locations and digitally less literate users struggle more to regain control. For some, a breach is just an inconvenience but for many, it can deeply interrupt our everyday life.

These patterns reveal that cyber vulnerability is no longer just a technical risk but a social condition. As more of identity, work and relationships move onto digital platforms, cyber harm increasingly reflects broader structures of power, inequality, and institutional trust. In a world where so much of life unfolds online, protecting digital security is no longer just about better passwords or stronger firewalls rather it is about recognising cyber vulnerability as a form of *structural social harm* embedded within the very systems that organise contemporary social life.

-----*****-----