Akamai

It’s time to talk about cyberstigma

Foreword

Cybercrime is incredibly common. And with the rise of AI, it's becoming even more difficult to tell the difference between a genuine request from someone they know, and a scammer.

And yet, there's still a perception that if you are a victim of cybercrime - whether that's fraud, stolen identity, or a cyberattack on a business you use - you've done something wrong yourself. You've failed to protect yourself properly. It's somehow your fault.

This is far from true. Cybercriminals' tactics are getting more sophisticated by the day, from deepfaked phone calls to cloned banking websites impossible to distinguish from the real thing. In many cases, there's simply nothing a victim could have done to prevent it from happening. And when it does happen, the impact goes far beyond the pocketbook.

Research we've conducted for this guide shows that many cybercrime victims feel traumatised by what happened to them - nearly two-thirds to be precise.. They lose sleep, they feel embarrassed, they even feel a sense of stigma about what they went through, and want to hide it from others.

All this leads them to avoid the one thing that might help them recover better - talking about it. With family, friends, colleagues, or a mental health practitioner.

Fighting this sense of stigma around cybercrime is what this guide is all about. In it, you'll find new research that sheds light on this worrying trend, and professional guidance on how to overcome the mental toll that cybercrime takes on victims. The guide also offers readers some tips on keeping yourself more protected from cyber criminals.

100% prevention of cybercrime just isn't possible today. But my hope is that this guide will help people have better, more open conversations about cybercrime, the real impact it has on our psychological well-being and empower them to take action to keep themselves more secure.

Because if we talk more about cybercrime, we'll stand a better chance of fighting back.

Natalie Billingham
EMEA Managing Director, Akamai

01

About the research

Research: Spotlight on cyberstigma

Cybercrime can wreak havoc on individuals and businesses alike, with an alarming number of victims experiencing significant financial and emotional consequences. However, our research found that one of the most striking statistics is the emotional impact. Cybercrime doesn't just harm someone financially, it can deeply affect their mental well-being and leave lasting scars on their confidence.

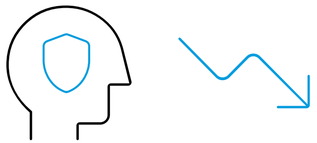
Methodology: The research was conducted by Censuswide, among a sample of 2002 respondents who have been a victim of a cybercrime (in the last 12 months) across the UK and Germany. The data was collected between 23.08.2024 - 27.08.2024. Censuswide abides by and employs members of the Market Research Society and follows the MRS code of conduct and ESOMAR principles. Censuswide is also a member of the British Polling Council.

71%

of victims admitted they felt "stupid" for falling victim to cybercrime.

Over half

of cyberattack victims experience a deep sense of shame.



Cybercrime deeply affects a person's self-esteem and sense of competence.

62%

of people who have been attacked experienced trauma.

50%

felt a toll on their mental health.

71% of victims admitted they felt “stupid” for falling victim to cybercrime and over half of cyberattack victims experience a deep sense of shame. Cybercrime can deeply affect a person’s self-esteem and sense of competence, even when the crime is often the result of sophisticated and well crafted scams.

62% of people who have been attacked experienced trauma and 50% felt a toll on their mental health, demonstrating just how pervasive the emotional impact can be.

More than half of respondents believed that hearing from other cybercrime victims would have prepared them better. However, many are reluctant to speak openly about their experience, with 41% hiding the emotional toll, and 43% avoiding discussing the incident due to fear of judgement. Only 29% felt comfortable informing their line managers at work.

The real reason why cybercrime goes unreported

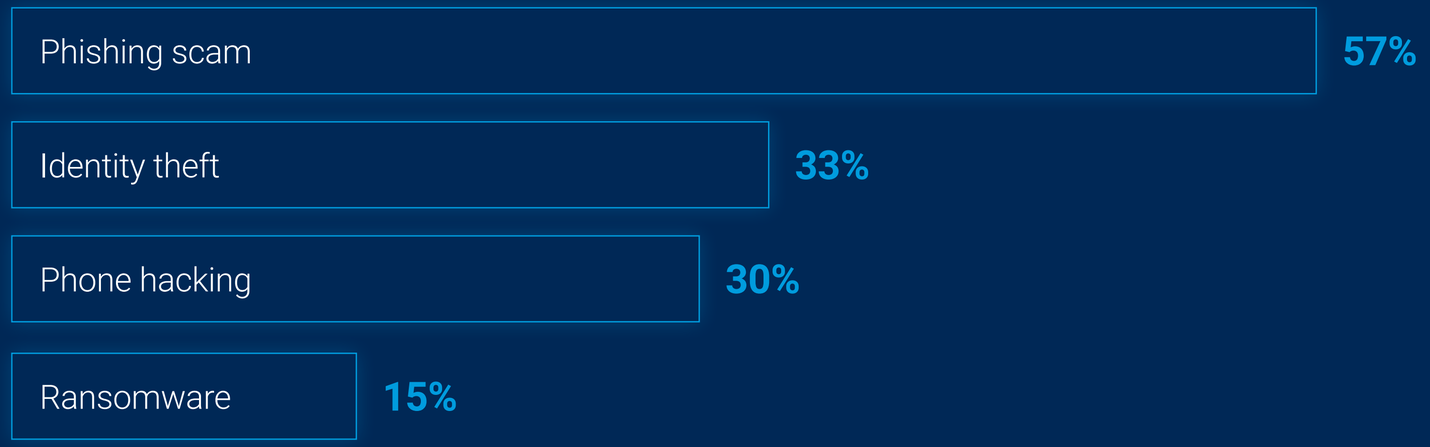
Where does cybercrime most commonly take place

79% of people reported experiencing cybercrime in their personal lives, while only 8% encountered it in the workplace. Within this, a worrying 13% of respondents were targeted both personally and professionally. Evidently, the comforts of home are leaving many people open to attack.

Phishing scams top the list of cybercrimes, with 57% of individuals falling prey to this type of fraud. In addition, identity theft, phone hacking, and ransomware attacks were also common.

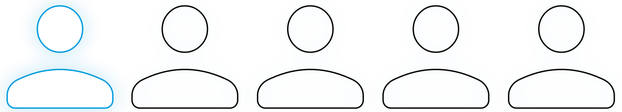
One in ten victims reported losing more than £1,000, with 43% losing over £200. As well as the larger sums, many fall victim to smaller, yet still impactful losses, with the most common financial loss being between £51 and £200.

Percentage of respondents admitting of falling victim to

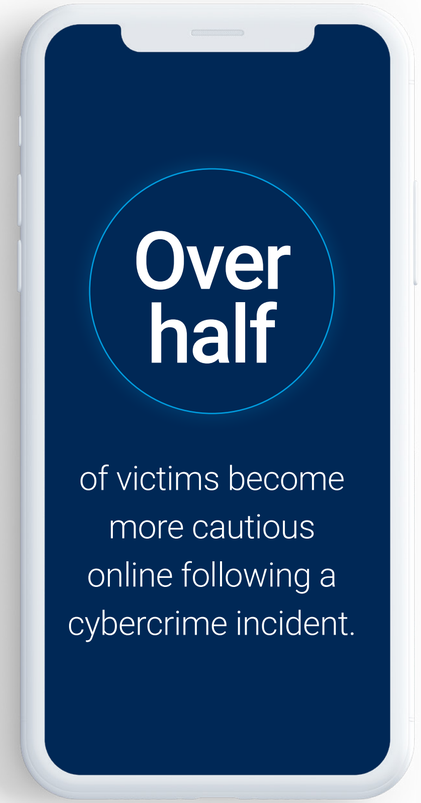


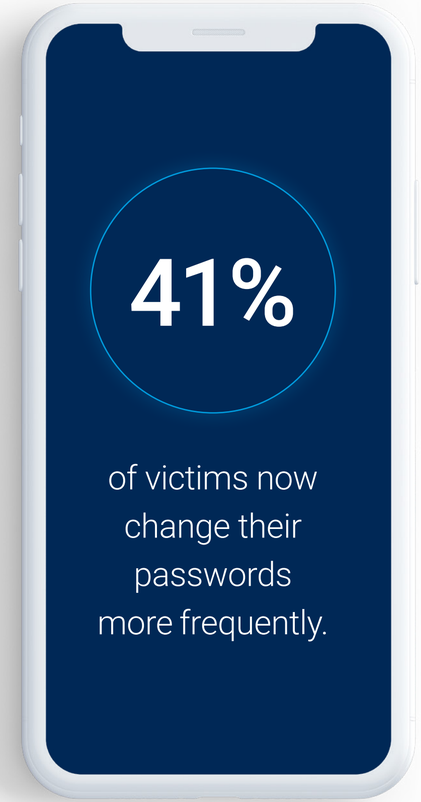
Life After an Incident

For many, the financial impact of cybercrime is long-lasting. With one in five people struggling to pay bills or meet financial obligations, and with some even reducing spending on essentials such as food and healthcare. A troubling 13% of people had to sell personal belongings, and 5% even lost their jobs.



In an effort to evade a repeat attack, following an incident many victims change their online habits.

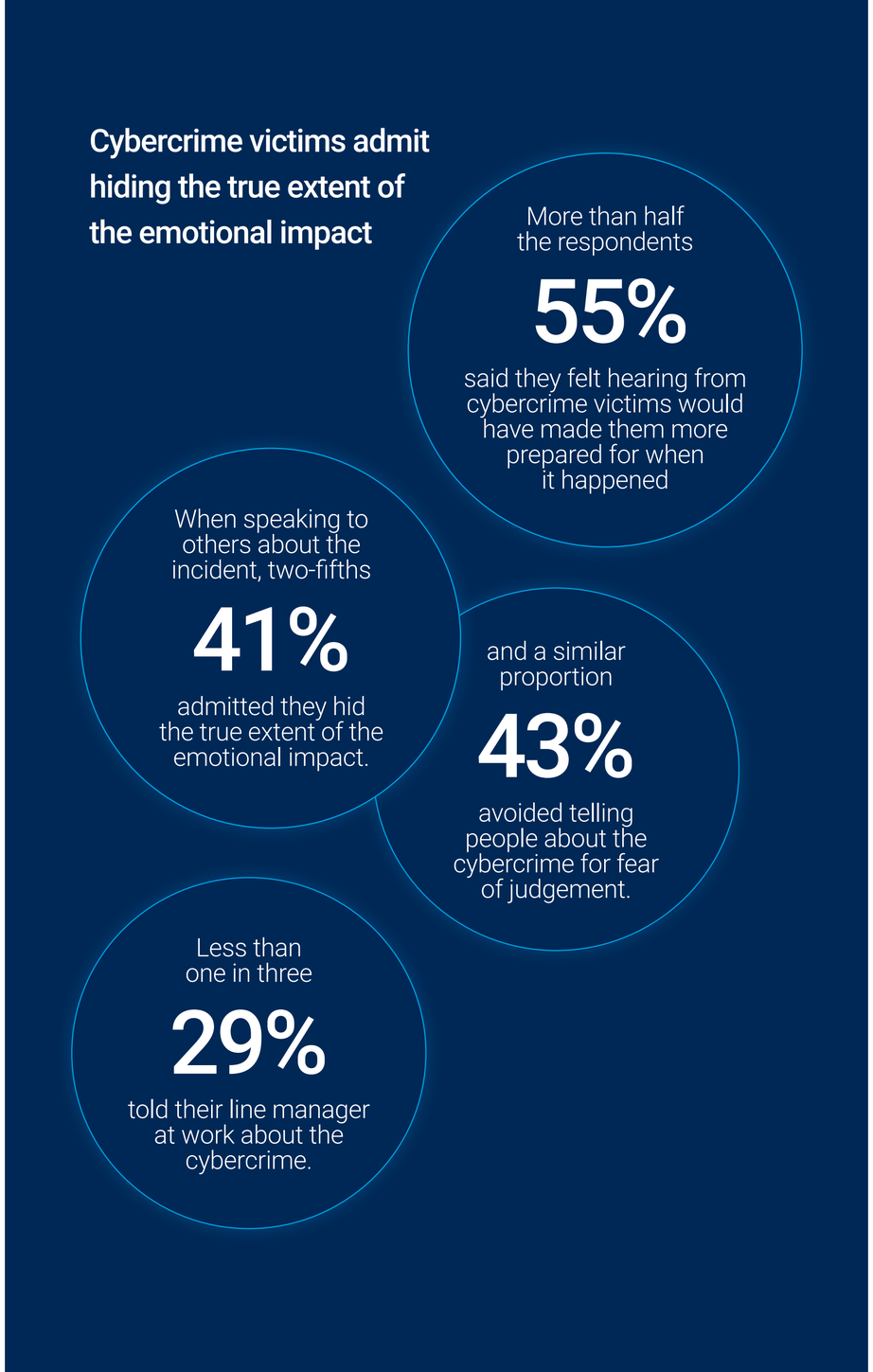




Victim Shame and Stigma

A majority of respondents feared becoming a victim again, while 51% felt they were unfairly stigmatised. Additionally, 61% believed the general public doesn't understand the full impact of being a cybercrime victim.

This needs to change. Talking about an incident helped many recover. 20% said speaking with family or loved ones made a difference, and 10% found written resources or advice articles useful in their recovery. Cybercrime has lasting effects, with 37% saying it took them at least a month to feel normal again. On average, victims needed around 10 weeks to fully recover.



Less than one in three (29%) told their line manager at work about the cybercrime.

Victims believe that more conversation about cybersecurity in the media and creating a culture of openness would help others deal with the aftermath of cybercrime. The need for more accessible information and support is clear.

> 1 in 3 victims think creating a more open culture around discussing cybersecurity would assist others in dealing with the aftermath of cybercrime.

It's not just a technological issue; it's a human one, with significant emotional, physical, and financial implications.

02

Mental health impacts of cybercrime

Dr Tara Quinn-Cirillo

The Mental Health Consequences of Cybercrime

In psychology we like to help people understand how their brain and body respond to the world around them. When we understand what happens and why, then this can reduce the impact and help us understand how to respond.

Our brains are primed to keep us safe. This can mean that at times we can respond in a more automatic and less considered way when we are in a difficult situation or one, we perceive as threatening.

Ideally, we can support people to 'catch' their automatic responses during times of threat and to move towards more considered or more purposeful action in response.

As this research has shown, cybercrime can be devastating on individuals' mental well-being. Our brains and bodies respond to difficult or uncertain situations by sending us negative thoughts and intense body symptoms.

Victims may find themselves asking:

"How did I let this happen?" - Self-blame is common, and feeds into feelings of inadequacy.

"Who can I trust?" - Being scammed can make a person feel betrayed, even if they've never met the perpetrator.

"I'm constantly on edge" - Many victims remain in a heightened state of alertness, fearing it could happen again.

"I'll never get my life back" - The losses, combined with the slow process of recovery, can make it feel like the damage caused by the cybercrime is permanent.

Prioritising mental well-being

But how can you prioritise mental well-being after a cyberattack, catching our automatic responses and move towards more purposeful action?

Acknowledge your feelings.

Accept that your emotional response is valid. Cybercrime is deeply invasive and can be traumatic. Bottling up emotions can worsen mental health. This is well researched and there are strategies and mechanisms available to help with this.

Take time away from other people.

When taking targeted time out, we engage in a short-term solitary time or an activity that does not involve other people. Targeted time out is proven to be good for our wellbeing, especially during times of crisis. This is different to avoidance or isolation where we may purposefully withdraw.

Limit exposure to further triggers.

If the cybercrime has occurred on social media, consider taking breaks or limiting your exposure to those platforms. Sounds simple, yet the impact is often profound and overwhelmingly positive.

Seek professional help where appropriate.

It is important to monitor the frequency, intensity and duration of your symptoms following cybercrime. You may notice that the impact is wide reaching across different areas of your life, or posing a risk to you in some way. Therapists, especially those familiar with trauma, can help you process the event safely. You don't have to go through this alone.

Establish a routine.

Rebuilding a sense of normalcy through routine can create stability in the aftermath of cybercrime. This can be as simple as maintaining a consistent sleep schedule or engaging in valued daily activities.

I know someone who has suffered a cybercrime. How can I help?

Those close to us play an important role on the impact of cybercrime on victims. It can be difficult to know how to talk about cybercrime, or even if someone is a victim. Here are some tips to help begin the conversation:

Don’t avoid the conversation.

It is natural to avoid difficult conversations. We may not know what to say when someone we know is experiencing a difficult time or is in distress. We can back out of a fear response; try and sit with any difficult emotions. You don’t have to problem solve. Simply holding a listening space can be impactful, by validating and not minimising their experience.

Create a safe space.

Make it clear that the victim can talk to you without judgement. Avoid comments like “How didn’t you see it coming?” or “I would have never fallen for that.” This is unproductive and it gives scammers the power to do more harm in the long run. Don’t force the conversation; sometimes victims just need to express their frustrations and fears rather than immediately fix the problem.

Acknowledgment & compassion.

Cybercrime can happen to anyone. Empathy can be your best ally even if you don’t fully understand what they’re going through. Validating feelings and experiences is important. Saying something like “it sounds like you’re feeling overwhelmed” or, simply “I am so sorry this happened to you” can be very helpful.

Offer practical support.

If you can, help them manage the practical side. Whether it’s assisting with reporting the crime, managing online security, or finding mental health resources all these things can be one less thing on their plate which can bring a sense of safety and comfort (tackling this together).

03

Best practice for cybercrime prevention

Richard Meeus

Improving your personal cybersecurity

Sadly, today cybercrime is a matter of when, not if. Knowing what to do after a cyberattack happens is almost as important as knowing best practice for preventing it from happening.

Cybercriminals have designed their tactics to exploit panic, complacency and trust. By understanding how fraudsters manipulate these emotions, you can make small changes to your online habits that will quickly improve your cyber-hygiene.

Always use a unique password

Using a unique password for every online account is a simple, easy and effective step that slows cybercriminals. This means if a cybercriminal discovers one password, they are not able to access your other accounts. Good quality password managers are a great way to help remember your many online credentials.

Keep your devices updated

Whether on your phone, laptop or tablet, install system updates when they're available. This ensures that security patches are implemented in good time and prevents your device from being left vulnerable with a known weakness that cybercriminals can exploit.

Assume every communication is suspicious

Thanks to AI, phishing attempts are only getting more sophisticated. So we can no longer rely on telltale signs that were previously a giveaway. Before you trust an unexpected text, email or website asking for your details, always look closely at who it's coming from, the email address, and website. Often, small changes can signal it's not a genuine message. Be especially wary of clicking on links, if unsure, open up another browser tab and go to the site directly if you have been before or check through a search engine. If you're unable to verify that a request is legitimate, do notNever give out sensitive information over email, text or phone.

Report the incident

If you've fallen victim at work, alert your IT department and report all suspicious communications. It may seem obvious, but less than a third of victims feel comfortable disclosing to their line manager that they've been targeted by cybercriminals. If you've fallen victim in your personal life, immediately contact your bank and credit reporting agencies and inform them that your personal details have been compromised.

Change all compromised details

If you have mistakenly given out sensitive information like a password or pincode, ensure these are changed as soon as possible. Use the opportunity to also update any old passwords and ensure they are all unique, robust and stored securely.

If you think you've been a victim of cybercrime, report the incident to Action Fraud, the UK's national fraud and cyber crime reporting centre:
0300 123 2040 | actionfraud.police.uk

These five steps do not require a lot of effort, but by implementing them, you can reduce your susceptibility to an incident and respond quickly and effectively in the event you fall victim.