Norton™ Cybercrime Report: The Human Impact


DANGER
HIGH
VOLTAGE

INTRODUCTION

Cybercrime has become a silent global digital epidemic. This shocking truth is uncovered by the Norton Cybercrime Report: The Human Impact.*

This groundbreaking study exposes the alarming extent of cybercrime and the feelings of powerlessness and lack of justice felt by its victims worldwide. It identifies people's intense emotions towards the perpetrators and the often flawed actions people take to prevent and resolve cybercrime. The study nails down the true cost of cybercrime while raising questions about people's own online ethics and behavior.

This report shows that every click matters. It highlights the need for better awareness and education for all Internet users and puts forward expert insights and advice on how we can take back the Internet from the cybercriminals.

More than 7,000 adults from 14 countries** took part in research for the **Norton Cybercrime Report: The Human Impact**

*For the purposes of this report, cybercrime includes: Computer viruses/malware; online credit card fraud; online hacking; online harassment; online identity theft; online scams (eg fraudulent lotteries/employment opportunities); online sexual predation and phishing.

**Australia, Brazil, Canada, China, France, Germany, India, Italy, Japan, New Zealand, Spain, Sweden, UK, USA

THE SILENT DIGITAL EPIDEMIC
CYBERCRIME IS HAPPENING TO ALL OF US

Cybercrime has become a silent global digital epidemic. The majority of Internet users worldwide have fallen victim and they feel incredibly powerless against faceless cybercriminals.

THE SILENT MAJORITY

For the first time, this report reveals that nearly **two thirds** of adults globally have been a victim of some kind of cybercrime (65%).

Cybercrime hotspots where adults have experienced cybercrime include:

83% **China**


76% **Brazil/India**

73% **USA**

Computer viruses and malware attacks are the most common types of cybercrime people suffer from, with **51%** of adults globally feeling the effects of these.

In New Zealand, Brazil and China it's even worse, with more than **six out of 10** computers getting infected (61%, 62% and 65% respectively).

Adults around the world have also been on the receiving end of online scams, phishing attacks, hacking of social networking profiles and credit card fraud. Seven percent of adults have even encountered sexual predators online.

CYBERCRIMES EXPERIENCED GLOBALLY

Computer viruses/malware **51%**

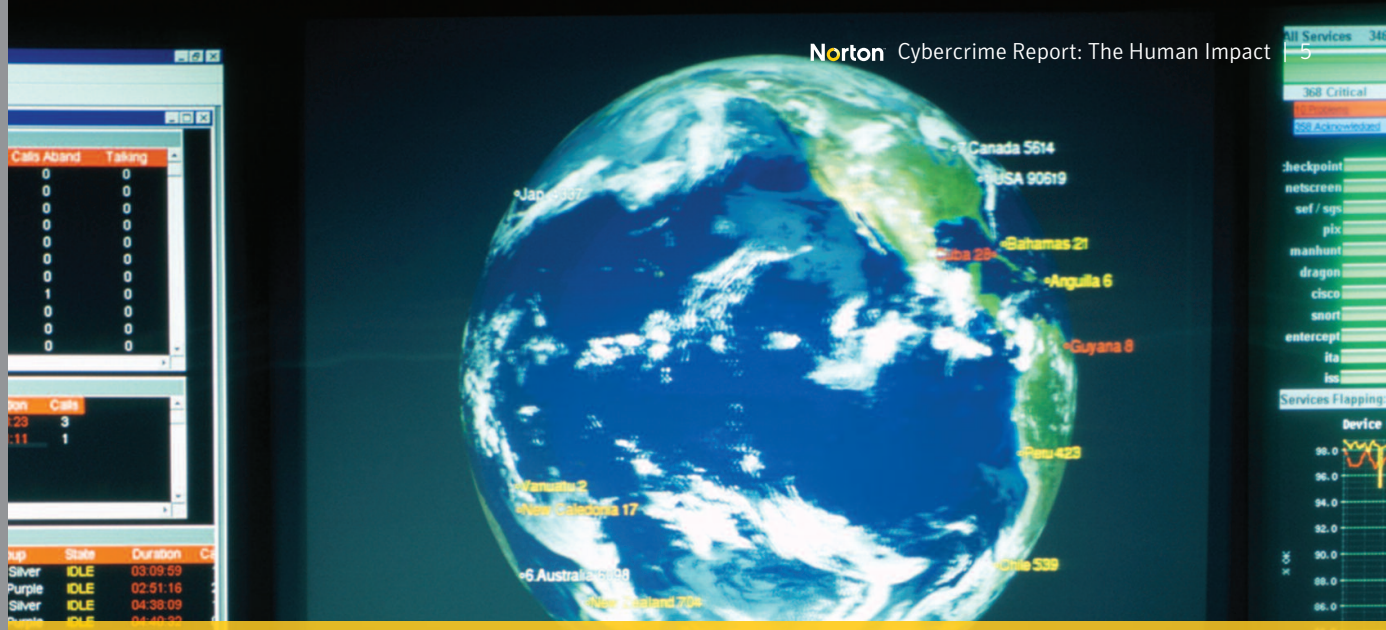
Online scams **10%**

9% Phishing

7% *Social network profile hacking*

7% ***Online Credit card fraud***

7% Sexual predation



"Computer and online crime is different from crime in the 'real world'. It's not tangible or visible to most people and hard to resolve. So it's vital to have up-to-date security software in place because, in the case of online crime, an ounce of prevention is worth a ton of cure." — *Anne Collier, Editor of NetFamilyNews.org & Co-chair of the Online Safety & Technology Working Group and Report collaborator*

“Every person has a weak point, the criminals are very sharp, they know when to strike.” — *Jagdeep, India*

PARALYZED BY POWERLESSNESS

It's sad but true that nearly **nine in 10** adults (86%) are thinking about cybercrime and **over a quarter** (28%) actually expect to be scammed or defrauded online. Only a tiny minority (3%) think cybercrime *won't* happen to them.

Yet despite the universal threat and incidence of cybercrime, only **half** (51%) of adults say they would change the way they behave online if they became a victim.

What percentage of people globally don't expect to be a victim of cybercrime?

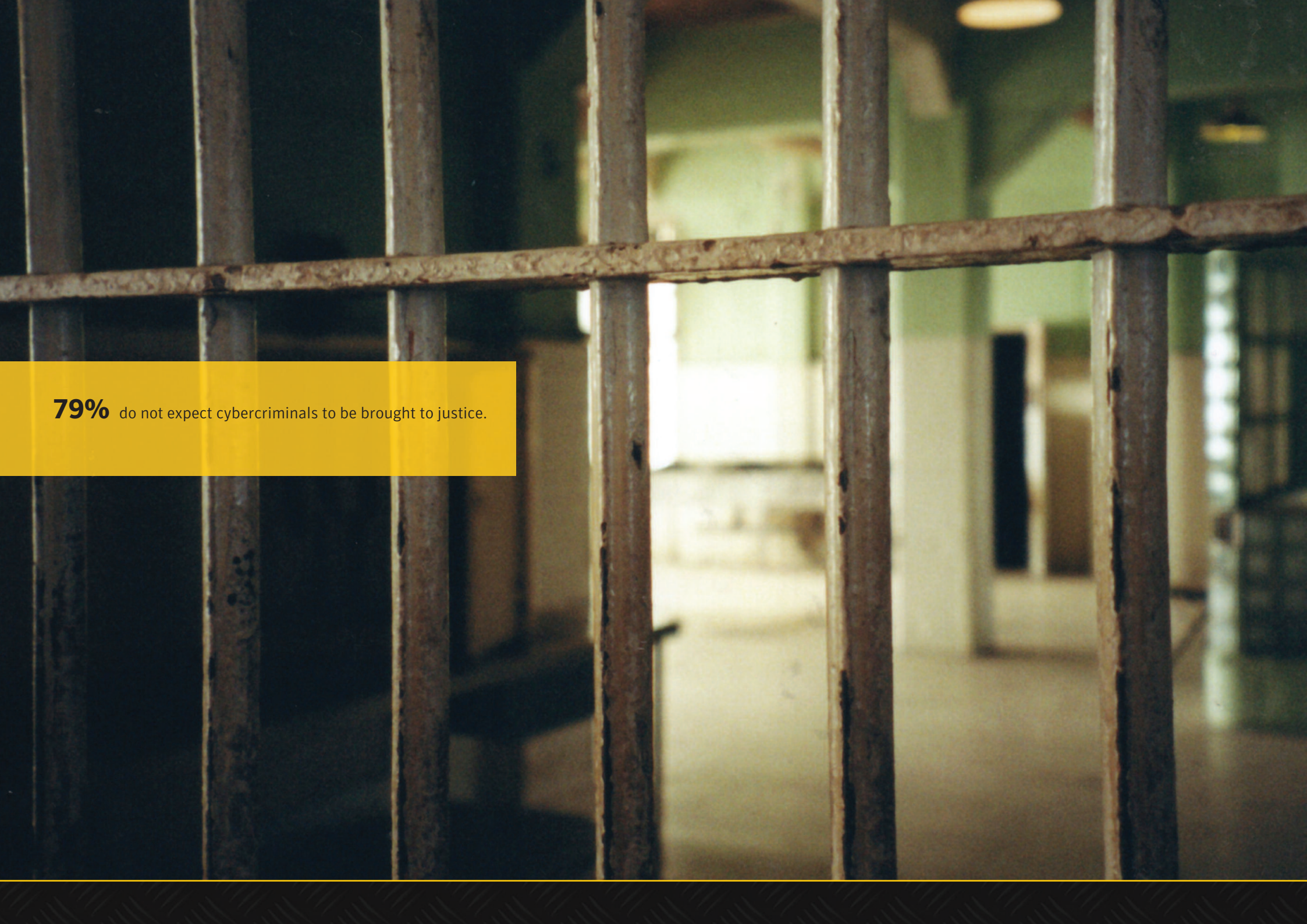
FROZEN BY FEAR

Why are we so accepting of cybercrime? According to associate professor of psychology at Loyola Marymount University, Joseph LaBrie PhD, it's what is known as 'learned helplessness'.

"Learned helplessness happens when people don't know enough about a problem or don't know how to resolve it. It's like getting ripped off at a garage – if you don't know enough about cars, you don't argue with the mechanic. People just accept situations, even if it feels bad."

And things are bad, with less than **one in 10** people (9%) saying they feel 'very' safe online.

> "You're eventually going to get some [virus or malware] after a while."
> — *Sandy, USA*



79% do not expect cybercriminals to be brought to justice.

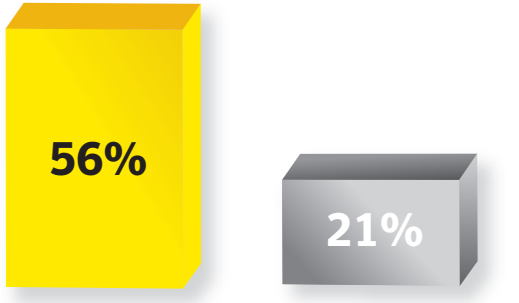
LACK OF JUSTICE AGAINST FACELESS CRIMINALS

Fueling the feeling of powerlessness is the belief that 'faceless' criminals are the main perpetrators of crime and almost **eight in 10** adults do *not* expect cybercriminals to be brought to justice.

Adam Palmer, Norton Lead Cyber Security Advisor, believes these figures tell a mixed tale. He says: "Many criminals reside in a foreign country so it's no surprise that people regard them as 'faceless' - they physically are. And because international cybercrime is hard to uncover and prosecute, people genuinely aren't seeing justice being done."

"But what shocks me more is the gap between the small number of people (21%) who think organized criminals are to blame for online crime and our existing data showing that 90% of today's cyber attacks are a direct result of organized crime."

Who's to blame for cybercrime?



> "Facelessness is scary. You can't explain it. It makes it harder to point the finger. There's nobody who knows who this person is."
>
> *— Todd, USA*

"I felt violated."
– Sandy, USA

"I wanted to get revenge."
– Suzanne, UK

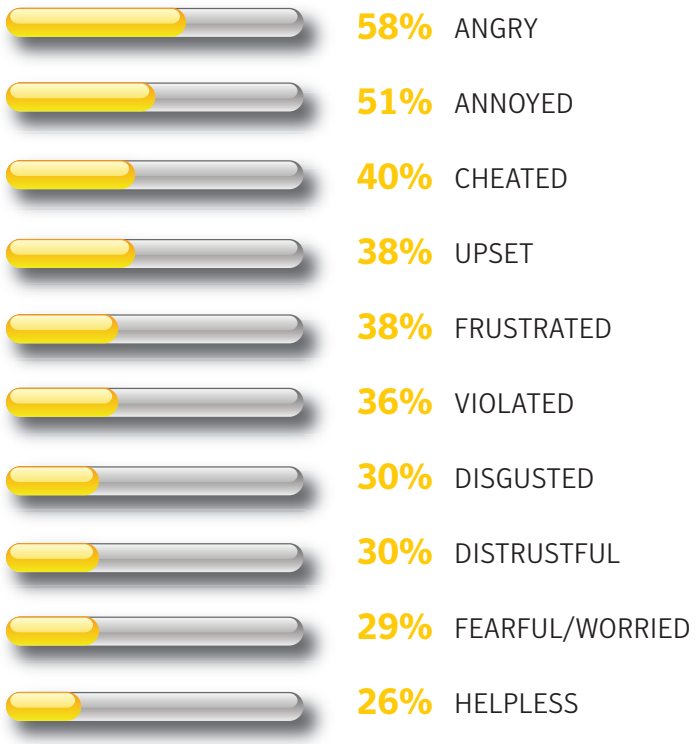
"I felt more angry than scared."
– Hana, Japan

PISSED OFF AND RIPPED OFF AND LEFT FEELING RESPONSIBLE

Adults all over the world are feeling angry, annoyed and cheated by cybercrime.

It causes intense emotions...

Top 10 emotional reactions to cybercrime



GRIPPED BY GUILT

When cybercrime strikes, individuals take it really personally and actually blame themselves for some cases of cybercrime.

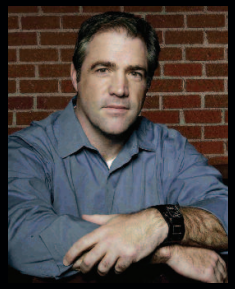
Even when it comes to online harassment or being approached by a sexual predator, some victims still blame themselves (**41%** and **47%** respectively).

Adults feel highly responsible for:

78%
Phishing

77%
Online scams

73%
Computer viruses/malware attacks



Joseph LaBrie PhD Associate professor of psychology at Loyola Marymount University

"These feelings are normal and realistic – they are the same feelings a victim in the offline world experiences," comments Joseph LaBrie. "But with an interesting twist ...

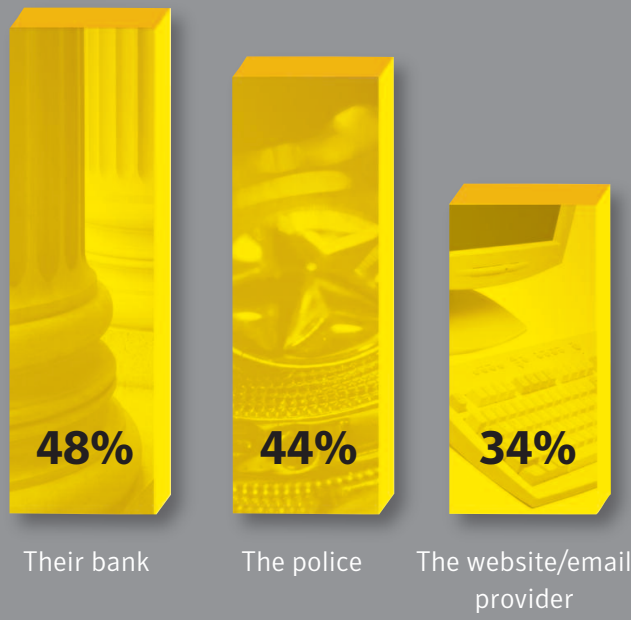
"We've developed certain expectations of technology that we haven't for other things. So when our basic right to use technology becomes complicated by cybercrime, we feel irritated because this is not how it is supposed to work!"

> "You start wondering how did this happen? You start blaming yourself and everyone else..."
>
> — *Kate & Walt, UK*

CALLING FOR HELP

When cybercrime strikes, **less than half** of all victims call their financial institution or the police and just over **a third** contact the website owner or email provider.

Who victims contact



In the UK and USA people are more likely to call their bank or financial institution (**63%** and **59%** respectively). While in Sweden and Japan, they are more likely to call the police (**74%** and **52%**).

GRASPING AT STRAWS

Around **a quarter** of victims take a DIY approach to resolving cybercrime. Unfortunately for them, our experts say the actions they are taking won't necessarily help them, and may not even be safe. For instance:

32% restrict the websites they visit

This only limits your enjoyment of the Internet. Security software with a search advisor tool will let you know if a site is safe.

26% get a family member or a friend to sort things out

Many threats go undetected by out-of-date or incomplete security solutions, so unless your friends are security experts, you will still be vulnerable.

25% try to identify the criminal and seek justice

Always work with law enforcement agencies, do not go it alone.

LOSING OUT ONE WAY OR ANOTHER

This study shows that resolution is hard to come by. In addition to hitting wallets hard, cybercrime is a major hassle for everyone around the world.

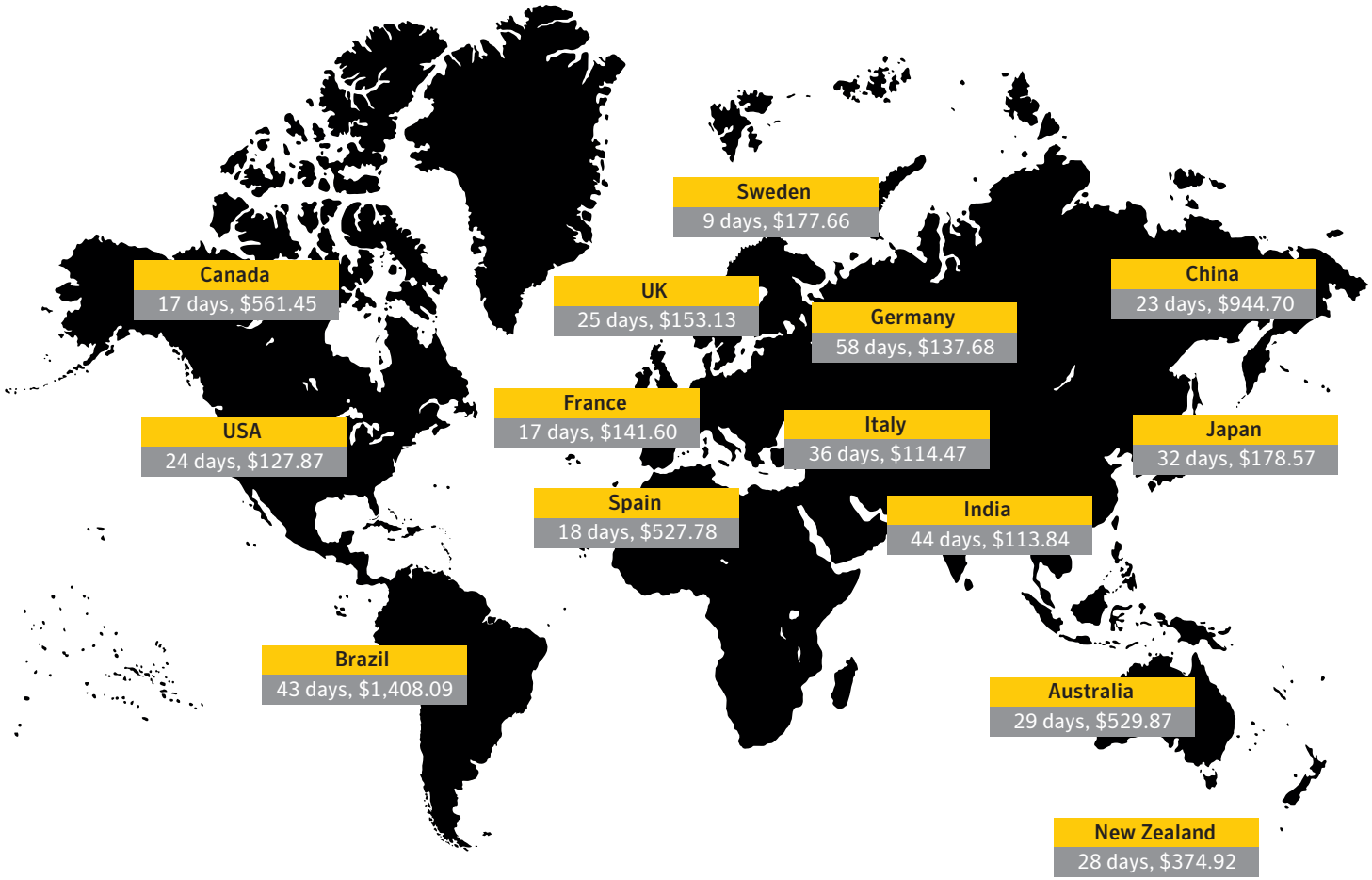
For nearly **three in 10** victims (28%) the biggest hassle is the **time** it takes to sort things out. Hardly surprising when you consider it takes **four weeks** to resolve an average cybercrime incident.

Then there's the emotional baggage, with around a **fifth** of victims finding it made them stressed, angry and embarrassed (19%), and **14%** mourning the loss of irreplaceable data or items of sentimental value, such as photo collections.

RESOLVING CYBERCRIME:

takes on average: **28 days**

costs on average: **USA $334***



Cybercrime costs time and money to resolve

*financial costs are quoted in USD

WE ALL PAY

"Even in countries where the individual cost of cybercrime may not be so high, we all pay in the end as financial institutions pass on the cost of their losses to all of us," notes Adam Palmer.

"Cybercriminals purposely steal small amounts to remain undetected. But all these add up. If you fail to report a loss, you may actually be helping the criminal because you are preventing law enforcement from knowing the full scope of the crime and being able to pursue charges."

NEVER RESOLVED

At the moment, nearly **a third** of victims globally (31%) say they never resolved a cybercrime.

Spanish adults seem to get the best deal with only **14%** of cybercrimes unresolved. This rises to **45%** in India and **49%** in China, but in Japan it's almost off the charts, with **60%** of victims never getting it fully resolved.

WHERE'S THE MORAL COMPASS POINTING ONLINE?

NOT TRUE NORTH!

"I am not stealing, you know ... I'm only downloading what is open to the world. I would be stealing if I were taking something from the supermarket ...the Internet is open, everybody downloads music, it's not only me."

— Mirela, Brazil

While people are justifiably angry about the bad guys and organized cybercriminals, this study also delivered insights that leave us asking 'who is the criminal?' The answers we received suggest many people's own moral compass is pointing in all sorts of questionable directions.

TEMPTED INTO UNETHICAL BEHAVIOR

The average man or woman in the street probably would never see themselves as a criminal, but in total **nearly half** think it's 'legal'* to download a single music track, album or movie without paying (17%, 14% and 15% respectively).

In addition to the musical moral maze, there seems to be a big grey area about online behavior towards individuals. While some people think it's perfectly okay to snoop, others wouldn't feel comfortable doing it – yet both would see it as legal.

Behaviors seen as legal*

30% Sharing or editing someone else's pictures

24% Secretly viewing someone's emails or browser history

17% Using someone else's research/work

FEW REGRETS

Despite these shaky ethics and questionable behavior, only **a fifth** of adults (**22%**) say they have online regrets. How come? Why is it so tempting to slip into unethical behaviors online? Is it the nature of the Internet? Psychologists believe so:

"We've become accustomed to getting so much of what we need off the Internet for free. So it's difficult to train people to think about paying for something in this otherwise free place. They don't regard it in the same way as regular commerce. The psychology around the Internet is that if it's out there, it's fair game." – Joseph LaBrie, PhD

WHY IT MATTERS

Norton's Adam Palmer says the number of people downloading illegal content is of real concern because it opens you up to more cybercrime:

"Cybercriminals are lurking in the places where people are downloading illegal content, and they're using those channels to distribute threats."

*Net 'legal' figures combine what people see as 'legal and perfectly OK' and 'legal but I would not feel comfortable doing so'.

WHITE LIES AND FALSE IDS ARE COMMON

WHO'S TELLING THE TRUTH?

Our study indicates that **nearly half*** of all people globally are happy to tell online lies about their personal details, including their name, age, financial and relationship status; their appearance and even their nationality.

And **a third** of all adults have assumed false identities online – from a false name through to a totally fictitious identity.

Lying and faking it online

33%

of adults have used a fake online identity

45%

of adults have lied about personal details

Germans are the best at faking it: **more than half** have adopted a fake online identity or lied about personal details online (53% and 51% respectively).

More than half of Chinese, Brazilian and Indian adults admit to lying about personal information online (58%, 56% and 55% respectively).

Around **four in 10** Italians, Brazilians and New Zealanders have also used false online identities (41%, 41% and 38% respectively).

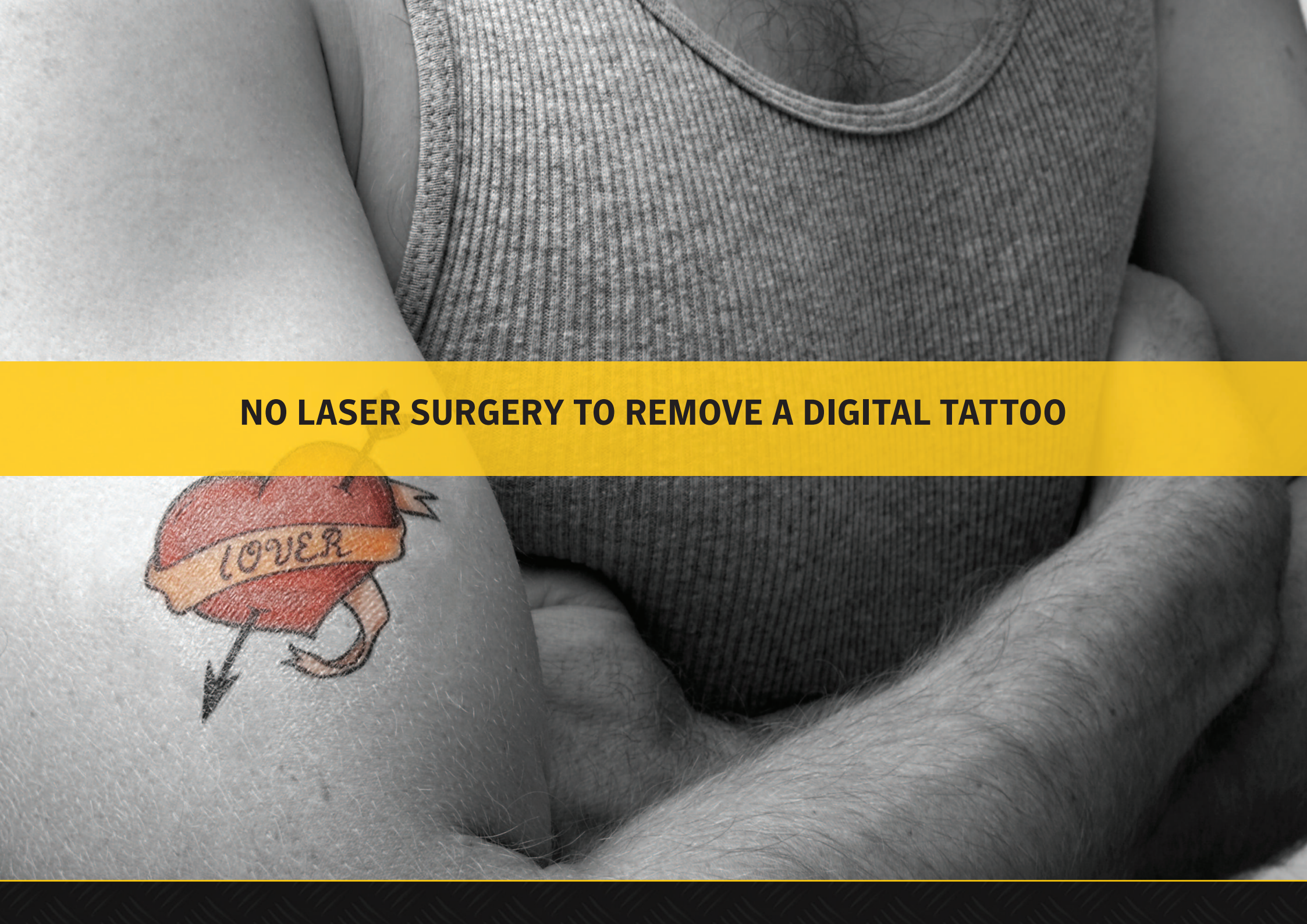
But people in the UK are reluctant to follow suit – they come out as the least likely to use a false online identity (**18%**) or lie about personal information (**33%**).

* 45% is a net figure of all those who have lied about personal details online

Anne Collier
Editor of NetFamilyNews.org & Co-chair of the Online Safety & Technology Working Group and Report collaborator

"Sometimes people create alternate identities or screen names online if they want to say something anonymously. Research also shows that users will fictionalize their social network profiles to fend off people who aren't their friends offline. Online anonymity can be positive or negative, protective or fraudulent. This study really brings out that – to protect themselves – people need to think critically about what they see and download as much as what they post online," says online security expert, Anne Collier.

"If everyone's faking it and telling white lies, do you really know who you are talking to? This could easily open you up to dangers online."



NO LASER SURGERY TO REMOVE A DIGITAL TATTOO

DIGITAL TATTOO

Nearly half of all adults globally believe you can never completely restore a negative online reputation (45%). Whether it's a bad photo posted online, a negative bit of gossip or even a self post that you later regret, online activity leaves a long, dark shadow.

And once you've sustained a damaged online reputation, it's like a digital tattoo – but with no laser surgery to remove it.

Canadian, Spanish, Australian and USA adults are the most pessimistic about restoring reputations – with **more than half** saying it can *never* be restored (57%, 54%, 51% and 51% respectively).

But it seems optimism lives on in China, where **only a quarter** (26%) fear they could never completely rebuild their reputations online.

> "I had to put in fraudulent information to get myself out (of the networking site), but I didn't care. Now if you search for me, it has bogus information." — *Kirby, USA*

DIGITAL RESPECT

Remaining optimistic and positive, the study also suggests that people seem to understand that being a good digital citizen is all about *respect*.

Personal rules, online etiquette and good manners are similar around the world. Only a tiny minority (**2%**) don't have any rules.

Global online etiquette rules

80% Don't harass or stalk people online

80% Don't bully or threaten others online

77% Don't pass along spam

74% Don't pass along embarrassing photos

ATTEMPTING TO PROTECT OURSELVES
BUT COMING UP SHORT

Fortunately, a lot of people around the world actively try to protect themselves against cybercrime by following some simple common sense rules.

Common sense rules

75% Never give out passwords

73% Don't give out personal information unnecessarily

71% Don't open attachments/links from strangers

69% Watch out for 'too good to be true' offers

69% Keep financial details safe and secure

Not so sensible...

However, our industry experts are also quick to point out that some so-called common sense approaches, aren't always that sensible. For instance:

27% say to only visit sites of big brands you know.

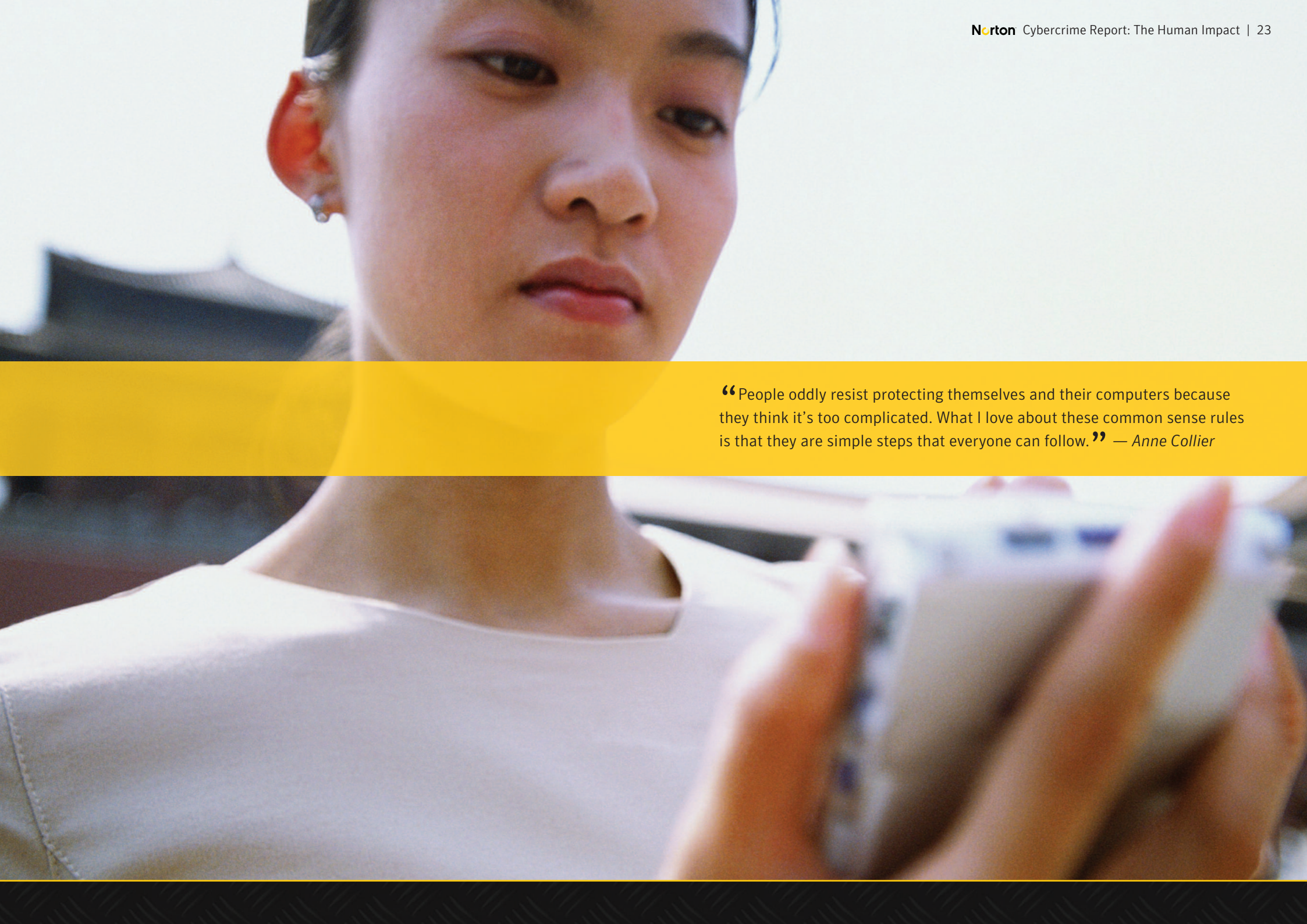
Even major brands come under attack. Use a security search advisor to know for sure if the site is safe.

29% say it's best to listen to recommendations from friends.

Cybercriminals hack contact books to send 'recommendations' of infected sites to 'friends'.

29% say you should look for the 's' after http in a web address.

These can be faked. Shop safely by using a full security suite not only an antivirus solution.



"People oddly resist protecting themselves and their computers because they think it's too complicated. What I love about these common sense rules is that they are simple steps that everyone can follow." — *Anne Collier*

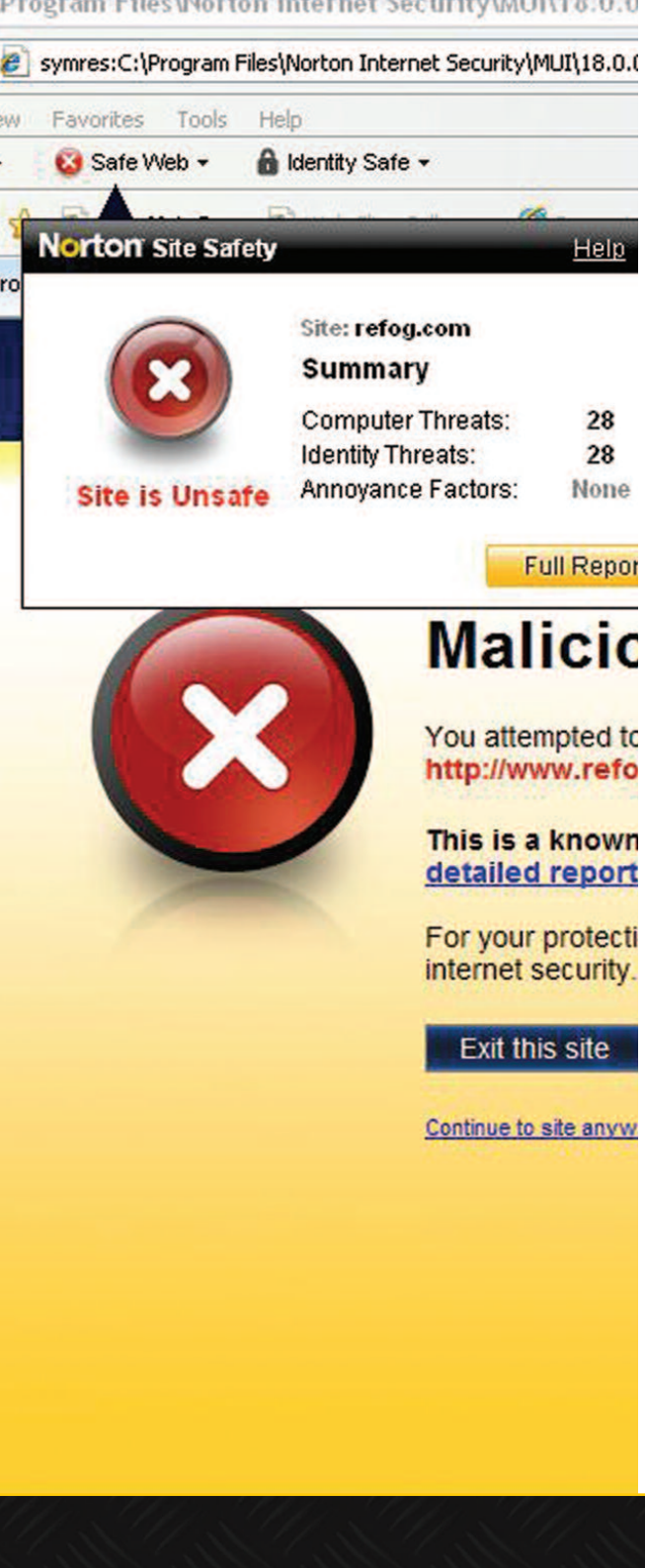
YOU ARE BEING SOCIALLY ENGINEERED TO ‘CLICK HERE’ AND FALL FOR CYBERCRIME

COMMON SENSE RULES YOU CAN'T IGNORE

We are being socially engineered to 'click here' and fall for cybercrime. At the moment, too many people are making it too easy for the cybercriminals.

By following a few more common sense precautions, we can deny the cybercriminals and stop all sorts of bad things from happening.

Allow	Deny	
cybercriminals to unlock all your online accounts	**a cybercriminal an easy ride**	
83% of people do not use a separate email address for online purchases	*Use different email addresses for different accounts*	
a cybercriminal to clean out your bank account	**cybercriminals from getting to your cash**	
74% of people use a debit card for online purchases	*Use one separate credit card with a small credit limit*	
cybercriminals to erase all your computer files	**cybercriminals from destroying irreplacable data**	
69% of people do not back up files regularly	*Back up regularly (and use it as evidence, too)*	
a cybercriminal to guess your password	**a cybercriminal easy access**	
62% of people do not change passwords frequently or use complex passwords	*Use complex passwords for each online account and update them often*	
a cybercriminal to tempt you onto a fake website	**a cybercriminal your click**	
60% of people do not use a browser search advisor	*Surf the Internet safely with the right security software*	



TAKE BACK YOUR INTERNET FROM CYBERCRIMINALS... THE RIGHT SECURITY CAN KEEP THEM AWAY

Victims the world over need to start taking a stand against cybercrime. Combining common sense with the right computer software makes a massive difference to fighting cybercrime.

It's time to:

- stop being frozen by fear and turn embarrassment into empowerment
- report all incidents to the authorities so the true picture of cybercrime emerges
- support the global Internet community by taking individual actions. The safer you are, the safer others can be

Everyone can contribute. Common sense is free, but free security or just antivirus software is not enough. Cybercriminals are always looking to get around security software, so the more comprehensive your security suite, the better.

The right software keeps them away.

"I honestly can't get past it, and no-one here has. Norton has really killed our viruses."

— MOD3RN H4X3R, cybercriminal

"I think Norton has beat us hackers in this game."

— Dartz, cybercriminal

REVERSE THE DOWNWARD SPIRAL

STATS WE WANT TO CHANGE

It is unacceptable that:

65%

of people worldwide have been the victim of a cybercrime.

Only 9%

of people feel very safe online.

Only 3%

of Internet users think cybercrime won't happen to them.

Adam Palmer, Norton Lead Cyber Security Advisor

"We should all be able to enjoy the Internet without fear of victimization. Empowerment will occur by raising awareness of the issues related to cybercrime and educating people on best practices and the right products and technologies to prevent becoming a victim. We are committed to standing on the frontline of the fight against cybercrime to see these numbers shift for the better each year."

For more information, visit:
www.norton.com/cybercrimereport

METHODOLOGY

The Norton Cybercrime Report: The Human Impact is based on research conducted between February 2-22 2010 by StrategyOne, an independent market research firm, on behalf of Symantec Corporation.

StrategyOne conducted an online survey among 7,066 adults aged 18 and over in 14 countries (Australia, Brazil, Canada, China, France, Germany, India, Italy, Japan, New Zealand, Spain, Sweden, United Kingdom, United States).

The survey was conducted in the primary language of each country. Questions asked were identical across all countries. The margin of error for the total sample of adults (N=7,066) is + 1.16% at the 95% level of confidence.

Quotes from individuals are taken from international qualitative research conducted by Infinia Foresight during November 2009.

CONTRIBUTORS

Expert insights, advice and tips have been provided by:

Joseph LaBrie, Phd, Associate Professor, Psychology & Director, Heads UP, Loyola Marymount University.

Anne Collier, Editor of NetFamilyNews.org & Co-chair of the Online Safety & Technology Working Group and Report collaborator.

Adam Palmer, MBA, JD, Norton Lead Cyber Security Advisor.

COUNTRY DATA

Each data sheet highlights country-specific information about cybercrime and the particular impacts on people in each country.

Data sheets for all 14 countries surveyed are available from:
www.norton.com/cybercrimereport


Norton™
from symantec

Symantec Corporation
World Headquarters
350 Ellis Street
Mountain View, CA 94043, USA
+1 (650) 527 8000
www.symantec.com

Norton™