FORTRA

Ipsos

FROM DATA PROTECTION TO CYBER CULTURE

End user awareness at the heart of cybersecurity challenges

TABLE OF CONTENTS

Introduction

This report aims to provide the basis for a discussion about developing a culture in which people know the cyber security risks of digital technology and its uses. We do this by looking at current levels of cybersecurity awareness among the working population in France, Canada, the US, the UK, and Australia. Before beginning, let's set clear parameters that define when an individual or group has developed a cybersecurity culture. In short, a cybersecurity culture exists when individuals can consistently identify and report potential cyberattacks and are aware of existing methods to prevent attempted intrusions. Cybersecurity culture is a subset of digital culture or "web culture."

For more than two and a half years now, terms like "cyberattack," "ransomware," "cybersecurity," and "phishing" have been appearing constantly in the media, in companies' internal and external communications, in politicians' speeches, and on social media. The Covid-19 crisis finally seems to have made "cyber-awareness" a tangible reality, although only to a limited extent. Hackers, meanwhile, have become ever more professional.

In 2021, ANSSI's threat report highlighted a 37% increase in the number of discovered intrusions compared with 2020, which is above the 1,000 mark. And judging by recent front-page news articles, it is very likely that the 2022 report will soon show a further increase in risk. As attacks have continued to increase, one cause has been involved in more than 90% of cases: human error or lack of attention. Although sophisticated techniques such as DDoS attacks exist, many attacks use and abuse "social engineering" processes and are based on a lack of cyberculture among individuals, along with strategies involving psychological pressure tactics to steal the data, money, and identities of consumers and professionals alike.

The nature of threats has also changed due to the advent of hybrid working arrangements that are still in flux, which has led to a recently identified phenomenon known as "Shadow IT." This term refers to the use of hardware and software by a company's employees without the agreement of their IT department. In 2020, the shift to 100% working from home was a severe test of IT security policies and highlighted the lack of knowledge about best practices. The situation still does not seem to have been resolved.

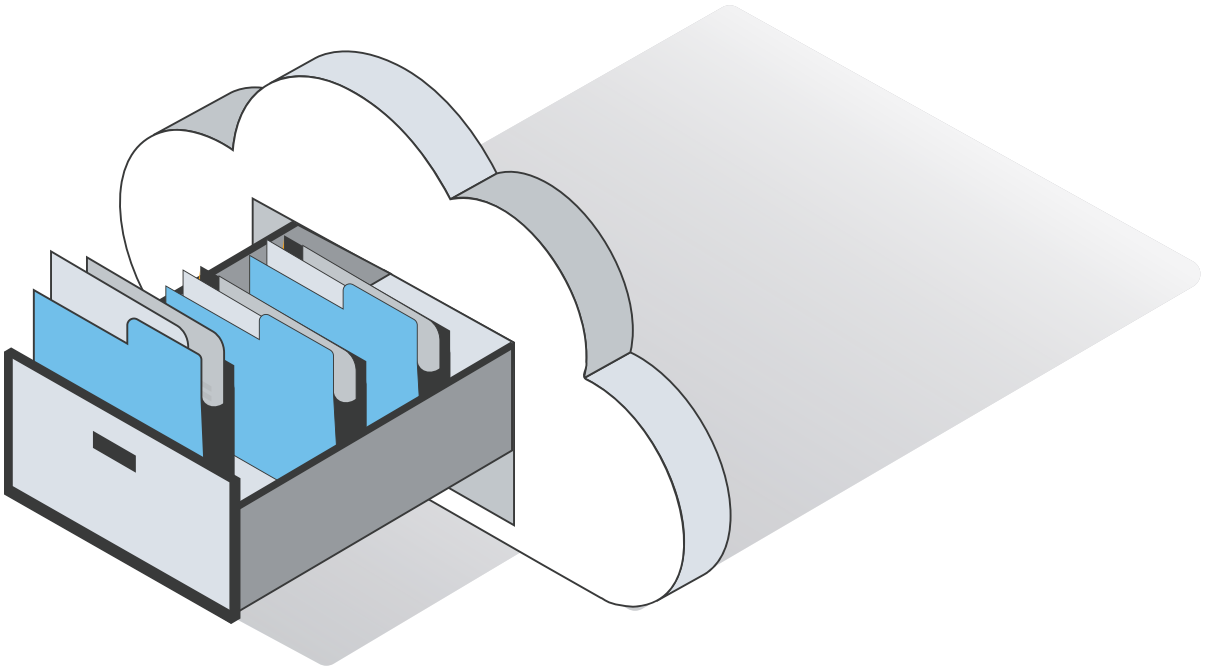
Accordingly, a key question is whether the increased visibility of cyber risks among the population has led to increased awareness or knowledge.

To answer this, it is important to remember that each human being can act as an effective shield against cyberattacks provided they are informed and prepared and have the necessary tools and support. Studies and reports on simulated attacks, such as the Gone Phishing Tournament Report, highlight a close correlation between the adoption of cybersecurity awareness programs and a "cyber" mindset among individuals.

According to the 2021 edition of this report, only 29% of institutions in the education sector, for example, had adopted awareness-raising and attack simulation initiatives, while 27.6% of people who received the phishing simulation email clicked on the link within it (as opposed to 19.8% on average among all respondents).

Given that cybersecurity awareness has made significant gains in terms of the importance organizations are placing on it internally, the minimum level of knowledge required for the average person to protect sensitive information has come under increased scrutiny.

As many familiar services, products, and shared experiences move from a physical to a digital space, adopting a cybersecurity-aware culture that can protect information against inherent technology-based risks is more crucial than ever. This process cannot succeed without integrating awareness efforts into our daily lives in a movement led by companies, public authorities, and the education sector.



Message from Dalila Ben Attia, Regional Director France, Terranova Security

For over 20 years, Terranova Security has worked tirelessly to ensure its clients have access to industry-leading security awareness training solutions. Raising awareness does not just involve teaching people about methods but also fostering a certain mindset in others. This means traditional eLearning content formats, which we have seen countless times in training sessions, are no longer sufficient. Simply launching courses and phishing simulations over the course of a calendar year won't guarantee the information is absorbed and acted upon. Continuous communication and reinforcement on key cybersecurity awareness topics are required to add cyber-aware behavior to your organization's cultural fabric.

It should be remembered that most individuals are not IT experts and that different generations coexist and may not share the same knowledge regarding digital technology. As a result, initiatives regarding cybersecurity awareness must be able to cater to those varying sensibilities while also ensuring everyone stays informed on what constitutes good online hygiene.

Building and growing a lasting security-aware organizational culture is an essential ingredient that will allow all technologies to secure confidential data in their personal and professional lives. While no one is immune from the consequences of a data breach, developing a cybersecurity culture is also the best starting point from which to reduce risk and strengthen layers of digital protection across all devices, files, networks, and systems.

This is why Terranova Security joined forces with Ipsos to analyze the current state of cybersecurity culture development in several major markets, to examine knowledge acquisition trends, and to see if individuals have, by and large, what they need to protect themselves against attacks. The results of the study **"Phishing, Malware, and Scams: The State of Employee Cybersecurity Awareness"** reflects this current reality.

This report sets out the major findings of the resulting research. It is a starting point for a discussion that we hope will be rich, inclusive, and a valuable contributor to helping your organization nurture its cybersecurity culture.

The State of Cybersecurity Awareness

IPSOS SURVEY RESULTS

The survey was conducted during the summer of 2022 among 4,000 individuals aged between 18 and 75 in five countries: France, the US, Australia, Canada, and the UK. The aim was to establish each person's interest level in and commitment to the topic of cybersecurity awareness.

With the rise in remote working since the start of the Covid-19 pandemic, have cybersecurity practices changed accordingly? To what extent do employees want to know more about best practices and implement them at work? What about in their personal lives?

High level of knowledge about cyber risks

The survey shows that almost 76% of employees in France, the UK, Canada, Australia, and the US say a cyberattack has personally targeted them or that they know someone who has. Alongside this awareness of the dangers, many respondents report that they have personally been the victim of a cyberattack. 72% in Australia and 61% in the US. In France, where personal and business cyberattacks have been huge news stories, 54% of respondents agreed with this statement.

The survey also highlights the French people's "weakness" in the face of attacks: 27% say they have personally been victims of a scam or an intrusion, as opposed to 14% in the UK. What about companies? What about respondents' colleagues, friends, and families?

More than one in three respondents believe that the level of cybersecurity knowledge in their company is average to good (34%). However, their assessment of themselves and their colleagues is harsher: 30% say that their personal knowledge is good, and only 22% say that their colleagues have a good level of knowledge, which suggests a lack of training and interest in this area. Fewer than 10% of respondents globally say that they, their company, and their colleagues have an excellent level of knowledge (i.e., have a score of 10 on a scale of 1 to 10). Therefore, this part of the survey shows a lot of room for progress from being aware of cyber issues to achieving fundamental knowledge.

"These results emphasize the importance of up-to-date educational training that raises awareness about security," **said Theo Zafirakos, CISO at Terranova Security.** "The survey results show that, although most people are aware of cyber threats and their prevalence across all regions and business sectors, we can assume that the overall level of knowledge is below average. The only way of making up that shortfall is to create an organizational culture that pays attention to security and introduces training that raises users' awareness and enables them to detect and report cyberattacks systematically."

Combating the growing challenges arising from remote working

According to the survey, 54% of employees work remotely, and 34% have been doing more since the Covid-19 crisis. While many people in English-speaking countries have adopted this practice, particularly those working for large corporations, France is holding out against the paradigm shift in working methods, with 56% of French people surveyed saying that they have never worked remotely. Among those experimenting with remote work arrangements, most—54% worldwide and 58% in France—state that they need additional IT support when working remotely to avoid cybersecurity problems. A significant proportion (37%) of respondents also said they pay less attention to cybersecurity when working remotely.

However, when answering the question about the rising level of attacks, respondents agreed, with 58% saying that phishing and scams have increased since 2020.

According to Anselme Laubier, account manager at Ipsos, "the jump in remote working caused by the Covid-19 crisis has strengthened the notion of shared responsibility for cybersecurity, at the corporate IT infrastructure level but especially at the level of employees, who can identify risks but still lack the necessary instincts."

Raising the question regarding the need for awareness training

Regarding cybersecurity awareness training offered by companies, the results are somewhat surprising, given that respondents in all countries say there is currently a cybersecurity emergency. In France, for example, ANSSI and Cybermalveillance.gouv have been working together since 2019 to alert people and raise their awareness about the risks they face when using digital technology. They have even produced user guides and set up an emergency phone number to deal with intrusions.

But what about companies? Has the state of emergency changed things?

According to the study, barely more than a third (38%) of those surveyed worldwide said that their company has set up a mandatory cybersecurity awareness program for all. The figure is higher in English-speaking countries but very low in France, where only 25% of respondents work for companies that have taken this action.

45% of French companies, according to respondents, offer no form of cybersecurity awareness training, whereas, in the UK, this is only the case for 31% of respondents. These figures are closely correlated with progress with training courses: only 29% of French respondents said they had completed a module, whereas the median for all the other countries is 49%. Australia came out on top, with 51% of respondents completing their modules, followed by Canada and the UK with 50%.

As reminder: levels of cybersecurity awareness training completion vary widely across countries and companies…

…by country and company size:

By country	Total	UK (n=500)	FR (n=500)	CA (n=1000)	AU (n=500)	US (n=1500)	1-49 employees (n=931)	50-500 employees (n=1271)	500+ employees (n=1798)
Started and completed Cybersecurity awareness training	45%	50%	29%	50%	51%	48%	22%	45%	59%

But, even if a company offers training, is there a reason why not all staff members participate?

"The three factors that influence employees' motivation to take part in security awareness training are accessibility, quality of content, and in-house reinforcement," added **Mr. Zafirakos.** "Do you offer your security awareness training in several languages? Is your learning content easy to digest, educational but also engaging? Do you continually reinforce the importance of cybersecurity awareness in-house using communication tools? These are just some questions that security officers should ask themselves if they see low training participation or completion rates."

For people who have never taken part in cybersecurity awareness training, two significant reasons arise from the survey: the fact that the training is not mandatory means that people are not motivated to participate. This revelation suggests that it is not a priority (as stated by 30% of respondents worldwide) except in France, where only 11% of respondents use this reason to explain their lack of participation.

The main reason for not engaging in awareness training, for more than half of respondents (53%), is they are not offered any training of this kind. The figure is highest in France, where 70% of respondents agreed with this statement.

This begs the question of whether the ongoing failure of many companies to offer cybersecurity training leads to a lack of interest among their people.

The answer is no: more than three-quarters of those surveyed (79%) state that they are interested in cybersecurity awareness training, even if their company does not offer it. However, cybersecurity awareness training does not seem to be a priority: one in four respondents worldwide believe that training is not necessary, with figures highest in Canada (27%), Australia (29%), and the US (27%). So despite growing interest arising from the increasing visibility of digital security issues, are companies including awareness-raising in their plans for the coming months and years? And above all, how do they get the most disengaged employees interested?

Anselme Laubier from Ipsos said, "remote working is still less common in France than in North America, the UK, and Australia. Logically, French people are the ones most keen on classroom-based learning."

However, although they are interested, they are not open to all learning formats. In the survey, respondents stated their preferences about how they learn about cybersecurity: practical activities such as phishing simulations (37% of respondents worldwide), online courses (37%), short game-based formats (32%), and sessions with an instructor (virtual or in-person) were preferred by more than 30% of respondents worldwide. France was an exception, with the latter category being in the first position, being preferred by 37% of respondents.

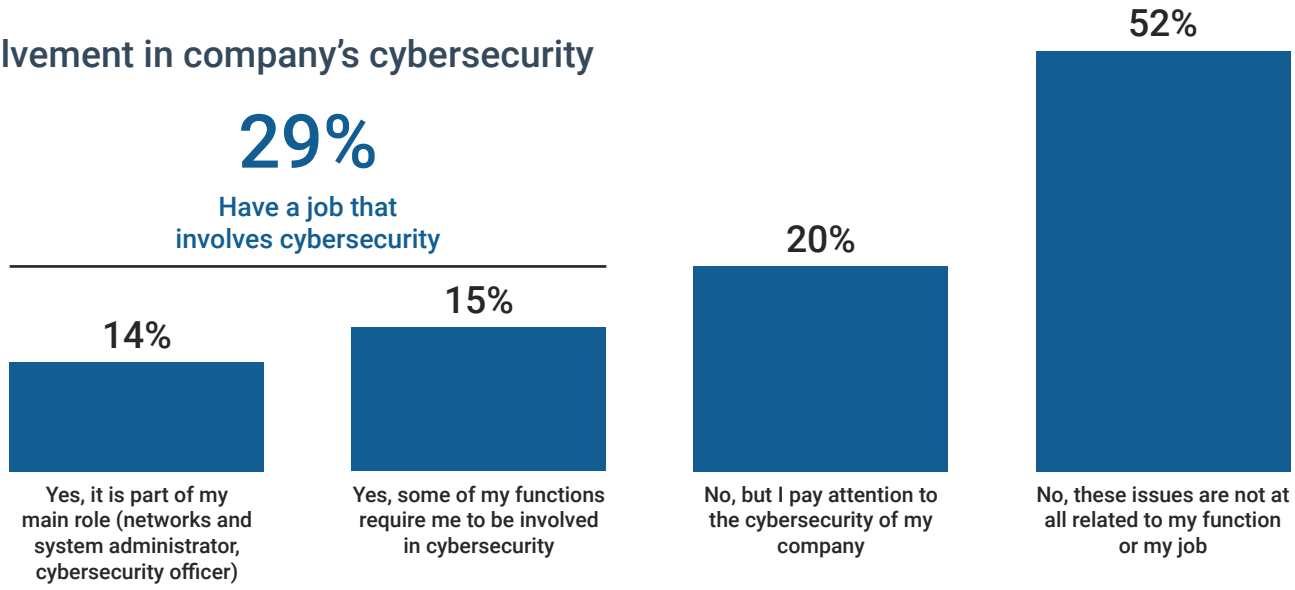
"It is clear that employees need security awareness training that is educational, relevant, and aligned with the organization's existing culture," said **Mr. Zafirakos.** "Even an audience that prefers sessions led by an instructor—virtually or in person—will not engage with security awareness content that adds no value to their day-to-day work."

And regarding responsibility for risks

For more than three-quarters (78%) of those surveyed, it is the company's job to ensure the security of all its employees. However, most (59%) also recognize that they are responsible for protecting their company in their day-to-day tasks and assignments.

52% say their job has nothing to do with cybersecurity

Involvement in company's cybersecurity

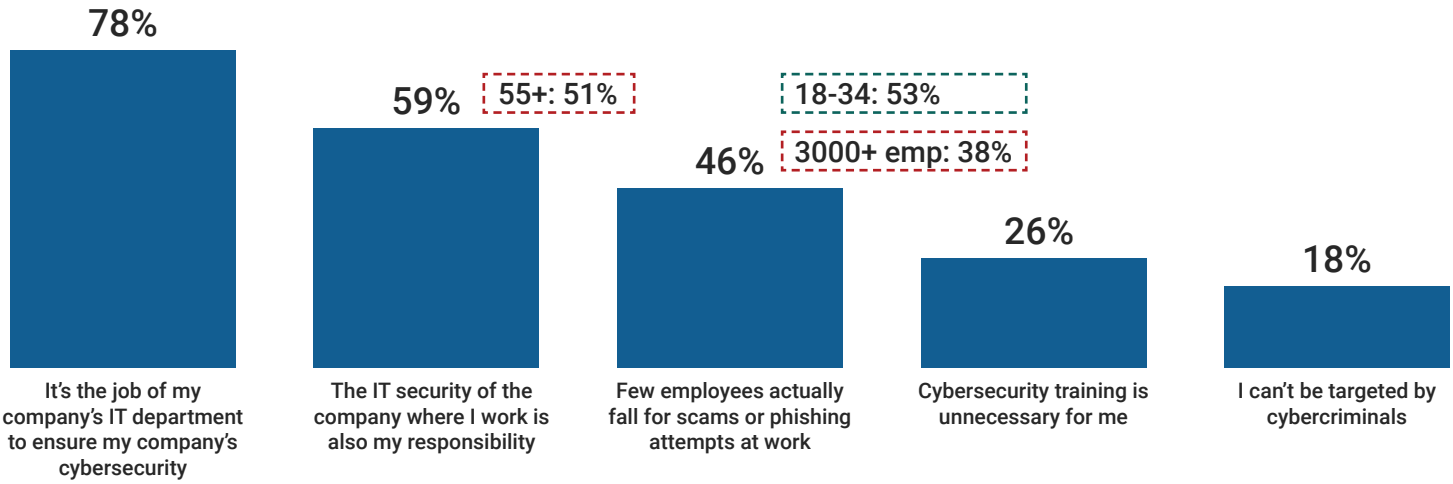


In your company, are you involved in IT support in cybersecurity ?

Base=4000: All answering No filters applied

A large majority relies on their IT department to enforce their company's cybersecurity… yet over half also feel (partly) responsible

% Agree re. Cybersecurity responsibility



To what extent do you agree or disagree with each of the following statements ?

Base=4000: All answering No filters applied

However, no other solution seems to be considered. Is this because people have a solid understanding of digital fundamentals? In France, 19% of people suffer from digital illiteracy, a figure similar to that found in the US by the National Skills Coalition Conversely, the OECD's latest global surveys on this topic have highlighted excellent levels of digital literacy in Australia compared with other markets studied, including France, the US, and the UK.

In 2020, the topic of digital illiteracy was discussed in the French Senate to encourage public and local authorities to take part in the action to close the digital divide (a concept mentioned for the first time in 1996) and combat digital illiteracy. Digital literacy should be understood as a body of digital knowledge, including basic skills (how to turn on a computer, how to do an internet search) and more advanced ones (using word processing and spreadsheet software, changing computer settings, setting up a WiFi connection, etc.). To borrow the expression used by Senator Raymond Vall, the challenge "can't be erased with just one swipe on a tablet!."

Is society in favour of a cyber culture that is shared by all?

Although not all respondents have received training in cybersecurity risks and issues, have they nevertheless adopted certain types of best practices? The answer is yes, which confirms the idea that a cybersecurity culture is slowly forming and can be strengthened by training. At work, a large number of those surveyed know the five basic principles of preventing an attack:

- Set up unique passwords for each account (50% but only 38% in France).
- Analyze emails closely to detect signs of phishing (47%).
- Be careful when receiving emails/texts (59%).
- Never click on links or open attachments in unsolicited emails and texts (61%).
- Report suspicious emails to IT teams (45%).

The only obstacle seems to be communication and the role people play in helping others: less than a quarter (24%) of people surveyed said they share best practices and discuss cybersecurity with their peers. However, if they fail to do so, their knowledge is less valuable because, by increasing the number of people aware of these issues, organizations can steer clear of an increasing number of ubiquitous cyber threats.

"While cybersecurity awareness has come a long way globally in such a short period, it's important to build and optimize programs with the present and future in mind," said **Mr. Zafirakos.** "The complexity, angles, and themes exploited by common threats are constantly changing as hackers try to gain the upper hand. Because of this, organizations and their security leaders must ensure security awareness training and reinforcement content is continuously evolving to include the most up-to-date information and guidance for employees to absorb and share."

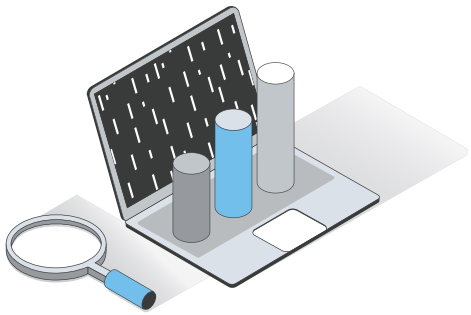
Outside of a work environment, those surveyed seem a little more willing to talk: 29% say they have discussed cybersecurity principles with others. Knowledge of best practices is also extensive, except for reporting, with people seemingly unaware that they can report scams to their messaging service provider, despite it being a practical step to take.

People seem to apply best practices more in their private lives, but why? Is the difference due to the fact that most individuals do not feel like custodians responsible for protecting their company's data, instead thinking that this is the job of their IT department? Or are they more cautious with their personal data because they feel naturally responsible for it?

This difference in attitude between the private and professional spheres cannot be attributed to a difference in threats, which are the same (data theft, viruses, scams, and phishing). The figures are indeed a little higher as regards personal cybersecurity. Still, as mentioned previously, this small gap can be explained by the relative inability of IT support teams to help staff members work remotely and safely when required.

So what are the key requirements for fostering a widespread cyber culture?

This study has highlighted several areas for improvement, starting with the general adoption of awareness initiatives at work. However, it is also essential to consider the sections of the population that have not yet joined the professional world. Extending knowledge and putting it within reach of everyone must form part of government action plans in line with current initiatives to compensate for cyberattacks. This topic has been widely debated in France since 2021. Although these insurance policies will help companies, individuals are still subject to the same dangers.



Three types of action are essential in order to foster this cybersecurity culture:

- Know the audience and determine its objectives
- Determine each person's specific risks
- Motivate all people to acquire the basics and share their knowledge

The foundations and emergence of a cybersecurity culture: how things currently stand

The aim of creating or helping to create cybersecurity and digital culture in 2022 may seem anachronistic. With all aspects of digital technology becoming widespread in our day-to-day lives, it is easy to imagine that most of the public already has the required skills and understands the underlying risks. However, the survey we carried out with Ipsos has highlighted that although people do not lack knowledge, they are at least guilty of not taking the topic seriously enough. The study also indicates that efforts to resolve the situation should not be limited to cybersecurity training and awareness-raising initiatives within companies. Such initiatives must extend to all, making everyone an ambassador who passes on knowledge.

DIGITAL ILLITERACY: THE SCOURGE OF OUR TIMES?

According to a study conducted by Insee in 2019, 17% of the French population did not have access to the internet and did not know how to use digital tools. In North America, the figure is around 20%, which is also seen in the UK, according to OECD studies. Only Australia—already top of the class in the Ipsos study—exceeds the level of knowledge defined as "good" by the OECD.

Efforts made by each country to tackle digital illiteracy and improve digital literacy among the population have begun only recently; they have usually been fast-tracked because of the changing nature of work and, therefore, the changing nature of the skills required. People often talk about a "new industrial revolution," which must be accompanied by a radical revolution in training, the knowledge economy, people's grasp of specific tools, and their development of the related culture. These last three aspects now almost systematically include digital technology.

In his most recent official speech at the International Cybersecurity Forum in June 2022, Guillaume Poupard, former head of ANSSI, addressed the topic of cybersecurity awareness as ANSSI's key challenge for today and tomorrow, and, more generally, for society as a whole to deal with the increasing role played by digital technology in our lives:

"The first thing we need to do is raise awareness of cybersecurity issues on a large scale. If we could have the attention of every French person for five minutes to get across a few digital security messages, it would be ideal."

If cyberculture is the most effective way of combating digital illiteracy, what are the prerequisites for successfully building the former?

Cyberculture has four main aspects, within companies and in society as a whole:

1. A strict framework and strict rules for defining the proper conduct for protecting against digital dangers
2. Education and training regarding digital risks, along with learning resources, allow everyone to acquire skills in this area
3. A clear statutory and regulatory framework regarding the rights and obligations of citizens, and companies, regarding digital usage
4. Standardization and explanation of technological tools to make them more accessible

The final aspect, which is harder to classify, concerns human beings. Everyone must be mobilized and targeted through their actions. Only by including individuals from all points on the security awareness knowledge spectrum can a security-aware culture genuinely emerge.

THE EDUCATION SYSTEM'S ROLE IN FOSTERING THE DIGITAL CULTURE

In France, the first courses addressing security in IT services appeared in the late 1980s (initially at the EPITA engineering school in 1989) but remained marginal until the early 2000s. Although STEM subjects have held an important place in education, specialization in cybersecurity is a recent phenomenon and remains rare. Coding lessons, for example, were only introduced in French secondary schools through the most recent reforms in 2019 and currently remain optional.

Although increasing the visibility of related professions seems to have become a priority for both the media and institutions, there remains a glaring lack of students taking these courses and of talent ready to be recruited into cybersecurity roles. A study carried out in France in December 2020 by software firm Kaspersky[1], regarding career guidance for young people and the appeal that cybersecurity careers hold for them found that only 12% of young people interested in a career in the digital sector were choosing to study IT security.

But in that case, how can we get young people more interested, if not to guide them towards careers in cybersecurity, then at least to raise their awareness of digital issues and make them as prepared as possible to deal with an increasingly virtual society?

The belief that education plays a crucial role and that education starts at school and continues in the workplace is a vital part of Terranova Security's DNA because of the backgrounds of the experts who make up the company.

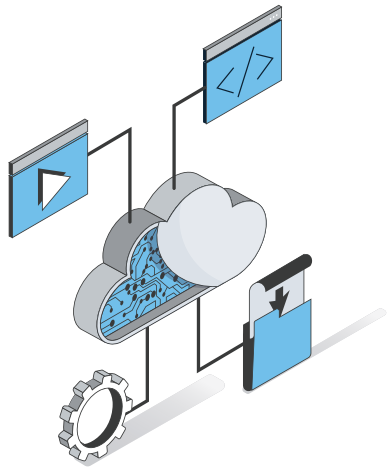
[1] "Préparer l'avenir numérique, c'est investir sur l'humain" ("Preparing the digital future means investing in people"), Kaspersky, January 2021.

"Training, awareness-raising, and the various initiatives that stem from them are things that people must know about and that must be carried out continuously," said **Mr. Zafirakos.** "To put this kind of learning in place, it is essential that public and private sector leaders commit to awareness-raising initiatives that inclusive and readily accessible."

This last point is crucial. By including each person in the process—which is also one of the main takeaways from the study carried out with Ipsos—you address existing interests in the subject and offer a response to the growing concerns many individuals have regarding cyber threats.

A THREE-WAY COLLABORATION BETWEEN THE PUBLIC AUTHORITIES, BUSINESS AND INDIVIDUALS

Fostering a security-minded culture is like building a house, with three key components providing strength to the overall structure: public resources, business, and individuals. Everyone has their role to play, at different levels.

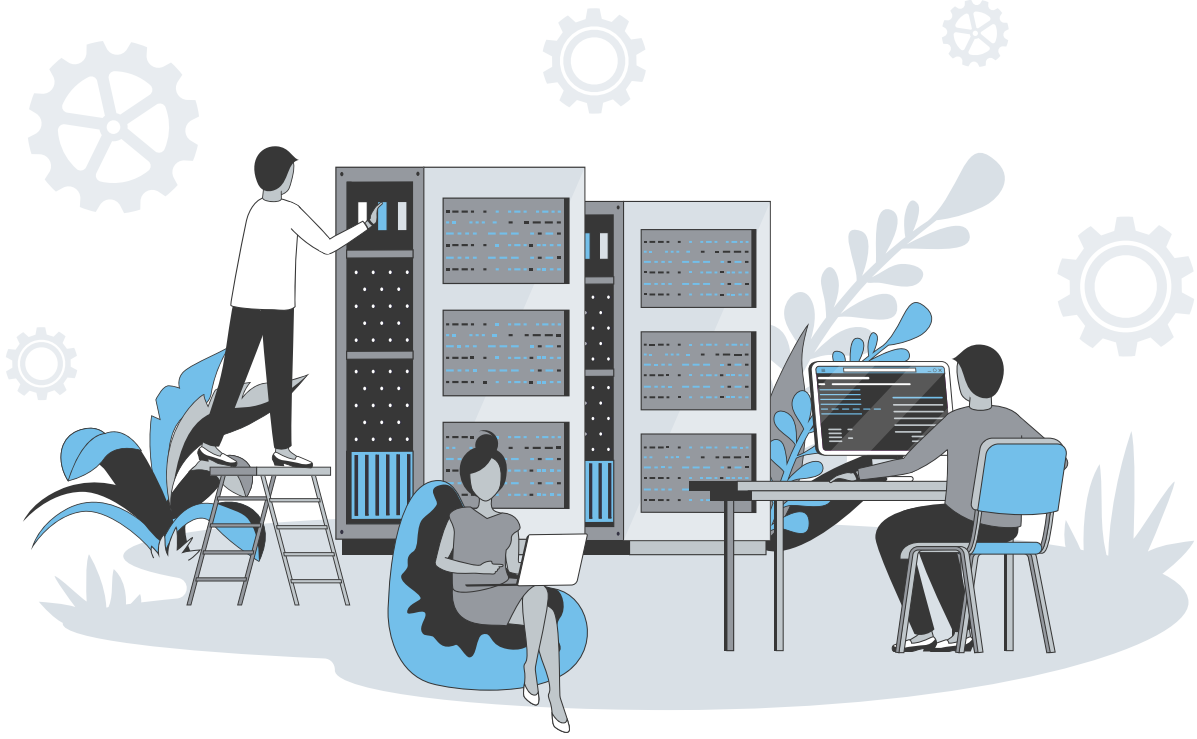


- The public authorities play a dual role: educating and protecting citizens by providing information, pushing through reforms regarding teaching and raising awareness of important themes, and providing tools.
- Companies and NGOs must become a conduit for knowledge by setting up training programs and adopting rules that allow staff members to develop a culture of addressing digital issues and using digital technology correctly.
- Individuals must engage and adopt a more responsible attitude to using tools, acting as digital evangelists among their friends and family, using social opportunities to share knowledge, and fostering a digital culture.

"Overall, certain areas of activity have already gone a long way towards setting up security training and awareness courses: companies with more than 500 employees, companies in the information and communication technology sector, the finance and insurance industries, and scientific and technical professions. In these areas, employees feel more concerned by the theft of sensitive business data and are more inclined to view themselves as custodians of their company's IT security. They are also more likely to share best practices regarding cybersecurity with those around them and to report live attacks to their IT department. Conversely, employees working in the retail, transport, tourism/hospitality, and real-estate sectors are not offered this kind of training as often. The result is that they feel less responsible and are less likely to report any attacks they encounter or share best practices with those around them," **says Anselme Laubier, Research Manager at Ipsos.**

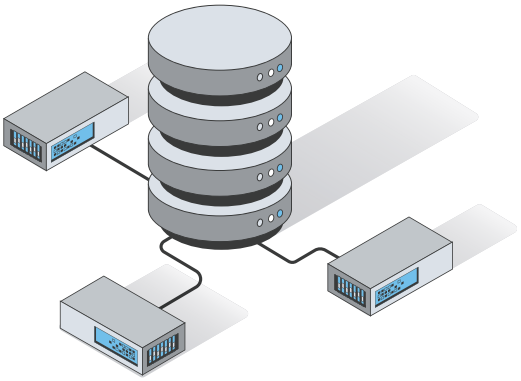
At a time when everyone is talking about digital natives and what they can contribute to society through their digital knowledge and skills—particularly in the world of work—it is important to remember that they are not the only people using the internet. In addition, although the younger generations are hyperconnected, they are not necessarily aware of the risks arising from their use of digital services, as shown by problems relating to cyberbullying, piracy, and the creation of fake accounts on social media. As a result, educating people, raising their awareness, or even teaching them the basics about digital technology concerns all generations, all socio-professional categories, and people from all backgrounds.

Numerous initiatives have arisen from these three main groups over the years, an example being Emmaüs Connect with its "Cahiers de l'inclusion numérique" ("Digital inclusion reports"), echoing the French 2018 act of the same name. More recently, the French government also set up "Cafés Transfo", places where people can discuss and share best practices, with the particular aim of speeding up the transformation of the public sector. This has been a significant source of inspiration and a key driver of change and engagement regarding digital technology. Digital user guides have also been developed, and courses showing people how to use digital tools have been introduced by local authorities to help all citizens.



And these initiatives specifically target audiences that share the same issues. However, the extent to which digital technology affects them may vary: the world is going digital, as is how we engage with it, and it is time we get used to it while staying safe. And progress does not appear to be slowing.

The urgent need for a joint base of knowledge about digital technology



Will we all be living in the metaverse? Are social media platforms taking control of our lives? According to a survey of significant trends in the next 25 years prepared by analysts at consulting firm Gartner, numerous technologies will influence people's working and personal lives.

For example, Web3, the metaverse, cloud computing, and—much more controversially—transhumanist technologies touch many crucial elements of the human experience. The latter phenomenon has nevertheless been developing for many years as a realistic vision of the future. As a result, we may be on the precipice of a world in which humans and machines are inextricably combined.

Instances of this transformation in action already exist. Pacemakers are a good example, as are subcutaneous NFC chips used in Scandinavia as part of the effort to digitize patient records. These connected objects, which include smart watches and TVs, are susceptible to cyberattacks.

While a cyberattack is irritating when it affects a standard IoT (Internet of Things) device, a smart implant is more dangerous if it can be controlled remotely. This topic is being taken particularly seriously by the European Commission, which, in mid-September 2022, adopted the Cyber Resilience Act, which tightens rules for producers of smart objects and software developers to prevent potential flaws and intrusions.

As well as IoT devices, another technical subject is often presented as a source of concern: artificial intelligence. Practical applications of AI—and their benefits for users—already exist and can be seen in our day-to-day lives. However, this cannot erase the impact of literature that highlights the potential for a war between humans and their more intelligent, stronger digital counterparts.

The most recent study on this subject, carried out in the US by Blumberg Capital, showed that half of US consumers are terrified of AI and its capabilities. And although AI-based "augmented humanity" applications have increased in the last three years, an article co-written by researchers specializing in AI and published by AI Magazine raises new questions about a form of AI that surpasses humans. Could it make humans inferior and almost force them to augment themselves to regain superiority?

These possibilities could become a reality and convince some people—if they need convincing—that we must adopt transhumanism and achieve a new global balance that is increasingly technological and connected. This would multiply the cybersecurity risks and the scope of attacks, which is already extensive.

But aside from the lack of information about cyber risks and people's fears about specific technologies, are there other factors that could hamper the development of cyberculture?

ARE TECHNOPHILES AND TECHNOPHOBES ALIKE INHIBITING THE DEVELOPMENT OF A CYBER CULTURE?

In his latest work entitled Homo Numericus, Daniel Cohen—an economist and professor at the elite French university Ecole Nationale Supérieure—discusses the usefulness of digital technology that "makes people more distant" and creates doubts among them, and more specifically, the psychological impact of social media and other virtual worlds on individuals. While social media and virtual worlds like Roblox and Fortnite have spread worldwide, particularly the younger generations—although the phenomenon varies between the world's regions—it seems clear that it is not synonymous with a security-minded culture.

The front pages of newspapers are full of stories about technology being misused and getting out of hand. Although this makes some people doubt the reliability of digital tools, it is not causing a sufficiently decisive change in mindset or even a behaviour change. Daniel Cohen's isolation seems to be a major factor hampering the emergence of a cyber or digital culture. When people spend too much time projecting themselves into virtual worlds, motivated by the desire to find a haven far from "real reality," there is increasing evidence to suggest that this hampers the social spread, and therefore the sharing, of knowledge, which is crucial.

This slippery slope, involving a passion for virtual worlds and a lack of knowledge about their intrinsic risks, is still something we have a limited understanding of, which is rarely addressed. However, it is mentioned in incident reports regularly published by antivirus software producers and ANSSI and in complaints made to CNIL and the police.

It is often said that there is a fine line between passion and hatred. While technophiles are not necessarily helping to foster a digital culture, technophobes are not helping either. Using the specter of a "big brother" state monitoring people's activities—which still looms large in people's imagination—and the threat of people losing their identity or even the meaning of their lives, technophobes are the objective allies of cyber-ignorance. France is frequently singled out for its supposed technophobia. It is often compared to the progressive approach of Germany and the UK neighbors: according to a December 2020 study, 56% of French people are increasingly concerned about new technologies[2].

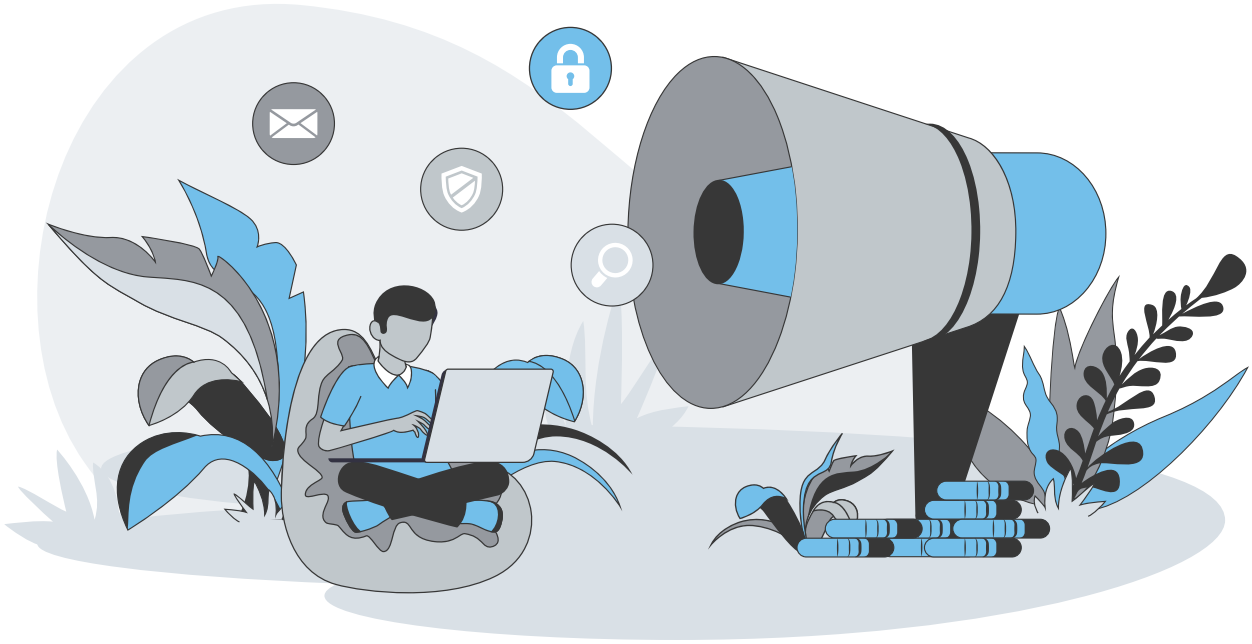
At a time when the world is constantly making progress and digital technology is increasingly integrated into everyone's daily lives, the behaviors arising from technophile and technophobe attitudes raise the question of how to respond. Is it a matter of inclusion? Or of communication?

[2] IFOP study for the Académie des Technologies, "Le regard des français sur les nouvelles technologies à l'heure des débats autour de la 5G" ("French people's views of new technologies in the context of discussions about 5G"), December 2020.

Conclusion

The survey conducted with Ipsos that is discussed in this manifesto provided the starting point for a broader investigation. In the final analysis, it is the responsibility of individuals to become—if they so desire—the ambassadors needed to create a cyberculture and to act as the heroes of their age. It is vital to give them a voice to measure their interest in cyber protection and, more importantly, their desire to commit to collectively rising to the considerable challenge of changing the course of history.

Many questions remain unanswered: how can their interest be piqued and maintained, what technologies and methods should be used, and what recognition will be given to these new skills in the future? It will be necessary to monitor and analyze these aspects in the coming months and years as digital strategies intensify worldwide.



ABOUT TERRANOVA SECURITY

Terranova Security is a world leader in cybersecurity training and awareness-raising and a partner of choice for businesses. Terranova Security's awareness-raising programs and phishing simulations provide organizations worldwide with the content of the highest quality, the most comprehensive security awareness platform, the most extensive portfolio of training and communication tools, and the most intuitive phishing simulator in the industry. Terranova Security works with security awareness-raising organizations and teams worldwide to devise programs that help to reduce the human risk considerably to provide an effective response to all kinds of cyberattack. Terranova Security is a member of Helpsystems, the global cybersecurity specialist. To find out more, visit the Terranova Security. website.

Press contacts:
Omnicom Public Relations Group for Terranova Security
Carla Portier–+33 (0)6 77 84 02 60
France.terranova-security@omnicomprgroup.com

ABOUT IPSOS

Ipsos is a world leader in market research and opinion polls, operating in 90 markets and with more than 18,000 staff members. Our researchers, analysts and scientists are passionately curious and have developed multi-specialist capabilities that allow us to provide in-depth information and analysis on the actions, opinions and motivations of citizens, consumers, patients, customers and employees.

Our 75 solutions are based on primary data provided by our surveys, our monitoring of social media, and our qualitative and observational techniques. Our tagline "Game Changers" encapsulates our ambition of helping all of our 5,000 clients navigate a fast-changing world with confidence. Ipsos was founded in France in 1975 and has been listed on Euronext Paris since 1 July 1999.

It is a constituent of the SPF 120 and Mid-60 indices, and is eligible for the deferred settlement service (SRD). ISIN: FR0000073298, Reuters ISOS.PA, Bloomberg IPS:FP www.ipsos.com

Notes

Notes

Notes

WWW.TERRANOVASECURITY.COM | WWW.IPSOS.COM