ERICSSON
CONSUMERLAB

ERICSSON

ONLINE THREATS GO OFFLINE

Understanding the effects of online threats in the physical world

An Ericsson Consumer Insight Summary Report
February 2017

CONTENTS

3. ONLINE ACTIVITIES IMPACT PHYSICAL SAFETY
4. A NEW THREAT REALITY
5. IN CONTROL
6. IN NEED OF SUPPORT
7. ON THE BRINK
8. ONLINE SAFEGUARDING MEASURES
9. TRUSTED FOR SAFEGUARDING ONLINE
10. STRENGTHENING THE ECOSYSTEM
11. PRIMING FOR A NEW REALITY

METHODOLOGY

The insights presented in this report are mainly based on data gathered from 27,668 face-to-face and online interviews with internet users aged 15-69 years old from July to September 2016. They represent 860 million people across 17 countries: Argentina, Brazil, Canada, China, Germany, Hungary, India, Italy, Japan, Nigeria, South Africa, Spain, Thailand, UAE, UK, USA and Vietnam.

Some analysis has also been included from the Ericsson ConsumerLab Analytical Platform, which covers data gathered from 24,760 face-to-face and online interviews with internet users aged 15-69 years across 21 countries: Argentina, Australia, Brazil, Belgium, Canada, China, France, Germany, India, Indonesia, Italy, Japan, Mexico, Netherlands, Russia, South Africa, South Korea, Spain, Sweden, UK and USA.

THE VOICE OF THE CONSUMER

Ericsson ConsumerLab has more than 20 years' experience of studying people's behaviors and values, including the way they act and think about ICT products and services. Ericsson ConsumerLab provides unique insights on market and consumer trends.

Ericsson ConsumerLab gains its knowledge through a global consumer research program based on interviews with 100,000 individuals each year, in more than 40 countries and 15 megacities – statistically representing the views of 1.1 billion people.

Both quantitative and qualitative methods are used, and hundreds of hours are spent with consumers from different cultures. To be close to the market and consumers, Ericsson ConsumerLab has analysts in all regions where Ericsson is present, developing a thorough global understanding of the ICT market and business models.

All reports can be found at:
www.ericsson.com/consumerlab

ONLINE ACTIVITIES IMPACT PHYSICAL SAFETY

The effects of what consumers do online increasingly have an impact on the physical world, from online shopping to working remotely, resulting in the blurring of online and physical activities.

This also applies to areas such as personal threats, and in matters related to health and finances. As a stark example, in 2016, an 18-year-old girl in Texas was bullied constantly on social media about her weight. Unable to bear the trauma, she took her own life. In fact, negative comments were being posted even after her death.[1]

Many have already experienced how online activities manifest as threats in the physical world – yet, thinking they know how to handle the situation, still feel in control of their safety. On the other hand, there are others who feel unsafe irrespective of whether they have had such experiences or not.

In this Ericsson ConsumerLab report, we explore how online activities can result in dangers in the physical world and how it relates to consumers' perception of safety.

KEY FINDINGS

1 A new threat perception is becoming a reality

- Almost half of the internet users surveyed say personal, financial and medical threats that originate online can manifest in the physical world.
- However, the other half still have a traditional threat perception and do not see threats in the physical and online worlds as interlinked. That said, their views are likely to be challenged in the future.

2 Those with the highest number of threat concerns also feel the safest

- Merely addressing threat concerns is not enough; the focus should be on supporting those who feel less in control.

3 Three in five internet users do not feel in control of their safety

- However, those who use multiple safeguarding measures have the greatest feeling of safety.

4 Consumers who feel safer have more trust in organizations to safeguard their personal data

- The key areas in which consumers need support are in preventing online identity theft and securing financial and contact information online.
- As online and offline threats are merging, safeguarding solutions that span both domains will become more important.

[1] CNN, December 2016, edition.cnn.com/2016/12/14/health/teen-suicide-cyberbullying-continues-trnd/

A NEW THREAT REALITY

We live in a world where 140 characters carry more power than ever before; where endearing Facebook profile pictures of a Beagle or Siamese cat incite racism and fuel hatred; and where whistleblowers can change the world, one tweet at a time.

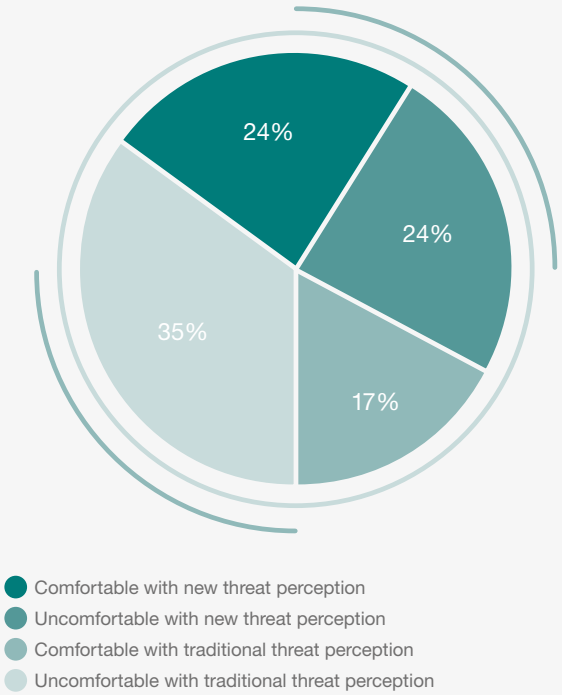
New media has given everyone the immeasurable power to go online and do anything – from shaming the most powerful of world leaders to helping a five-year-old cancer patient become a superhero for a day. It is precisely this unhinged revolution of free expression that is shaping a new threat reality.

This is a reality that encompasses every area of our life. For example, we do our holiday shopping online only to wake up one morning to realize that someone has used our credit card information to buy a pair of boots at a sports store in another country.

The medical industry is not immune either. With wearables being as popular as they are, your future employer could very well find out if you have a condition that will impact your employability.

And so, this revolution is marking a connection between threats in the online world and the physical world.

Figure 1: New and traditional threat perceptions



Source: Ericsson ConsumerLab, Online Threats Go Offline, 2017
Base: Internet users aged 15-69, 17 countries

A new threat perception

In this report, we explore a change in the perception of threats, primarily focusing on personal, medical and financial domains, and how different groups of consumers see online actions in these areas manifesting in the physical world.

From our research across 17 countries, we see that almost half of all internet users believe their online activities can result in threats or dangers in the physical world, a belief we refer to as a new threat perception. Conversely, people who perceive online and physical threats separately have a traditional threat perception.

We also split these two groups of consumers based on the extent to which they feel in control of their safety and end up with four distinct groups of consumers (Figure 1): 24 percent have a new threat perception and feel comfortable handling the new situation; another 24 percent have the same new threat perception but feel uncomfortable; and 35 percent feel uncomfortable even though they have a traditional threat perception. Furthermore, 17 percent still have a traditional perception of threats and feel comfortable with their safety. This group has low levels of overall internet activity and a correspondingly low level of concern for online threats.

Almost half of all internet users have a new threat perception

Threats to financial safety are top of mind for consumers. More internet users have a new threat perception when it comes to financial information, compared with the threats to personal safety and medical information. Forty-three percent of internet users say financial activities online are linked to financial dangers in the physical world. This is not surprising, given that financial transactions have moved online faster than other activities, but indicates a continued need to protect financial information.

IN CONTROL

The group we refer to as being comfortable with the new threat perception has a high proportion of advanced internet users, connecting to six or more internet services daily on any device. Fifty-four percent in this group go on social networks for an hour or more daily, compared to around 43 percent at an overall level.

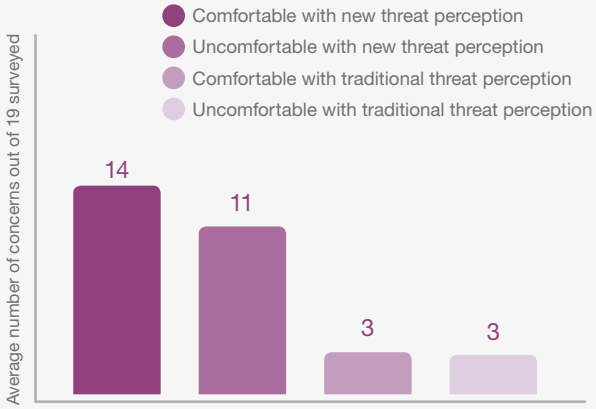
As many as three in five in this group live in bigger cities, in contrast with one in two at an overall level. Interestingly, in developed countries, 50 percent comprise white-collared professionals, compared to 35 percent at an overall level.

Though they feel in control of their safety, about two in three in this group still have a high number of concerns about personal, financial and medical threats, which is a greater number than those in other groups. This is important as it shows that judging threats based purely on concern is misleading – the group with the largest number of concerns is also the group that believes it can comfortably handle these threats (Figure 2), and therefore has the strongest feeling of safety. This suggests that the group that may express the highest level of concern may not necessarily be the one in the greatest need of safeguarding services. Rather, the priority should be to provide support to the groups who feel less in control.

Those comfortable with the new threat perception are primarily concerned about their financial information getting compromised and misused, as well as with online identity theft. Being a victim of social engineering is their second highest concern. This is understandable, given the sophisticated means that cybercriminals are using to swindle money today.

The group with the highest number of concerns also feels the safest

Figure 2: Number of threat concerns



Source: Ericsson ConsumerLab, Online Threats Go Offline, 2017
Base: Internet users aged 15-69, 17 countries

For instance, there are scammers claiming to be from e-commerce websites that email unsuspecting victims, inform them of a problem in processing their order, and ask them to resubmit personal and financial information. More than three in four of those who are comfortable with the new threat perception state that they worry about being a victim of such social engineering or phishing attempts.

Fear of ransomware attacks is also among the top 5 concerns for this group, with 76 percent expressing concerns about being a victim.

A constant online presence has meant that online bullying is having repercussions in the physical world. Interestingly, among those who are comfortable with the new threat perception, 76 percent of teenagers are concerned about

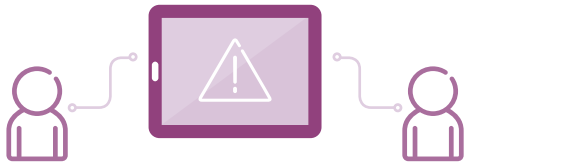
Figure 3: Top concerns of those who feel comfortable with the new threat perception

Source: Ericsson ConsumerLab, Online Threats Go Offline, 2017
Base: Internet users aged 15-69, 17 countries

IN NEED OF SUPPORT

The true measure of the new threat reality is attributable to how in control consumers feel of their safety. Twenty-four percent of internet users surveyed have, just like the previous group, started to recognize how online activities can result in threats or dangers in the physical world; however, unlike the first group, they do not feel in control of their safety. We refer to this group as being uncomfortable with the new threat perception.

This group is greatly concerned with different kinds of threats: 64 percent worry about online identity manipulation threats, and a similar proportion fear that someone might use malware to gain access to personal information.



13%

Only 13% of those who feel uncomfortable with the new threat perception feel in control of their safety in the online world

In 2016, a malware in the payment gateway of multiple Indian banking service providers lead to 3.2 million ATM cards being compromised, in one of the largest cases of hacking.[2]

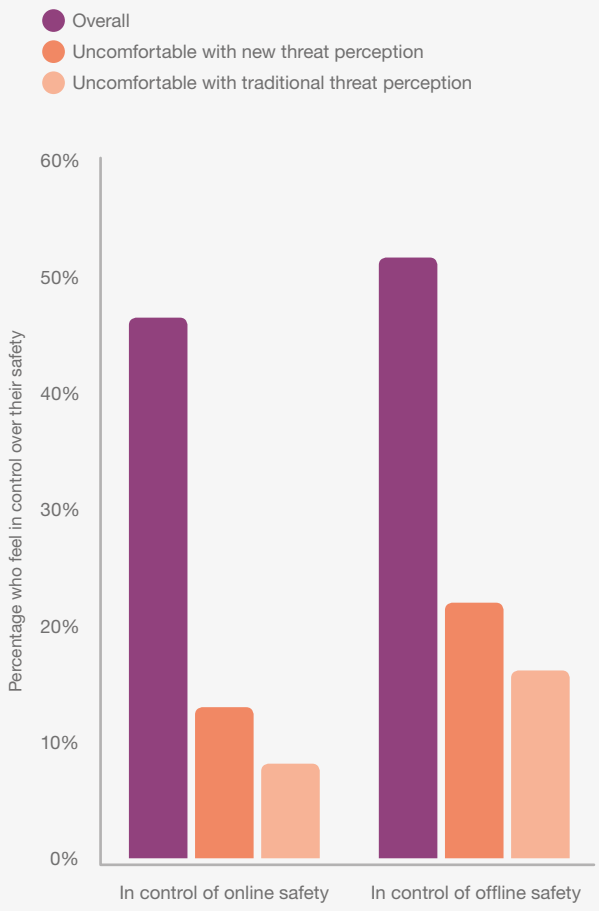
More than three in five worry about being a victim of ransomware, and a similar proportion fear social engineering or phishing attempts. This comes as no surprise due to the rise of such incidents in recent times.

A ransomware known as Popcorn Time was in the news recently. Once infected, the attackers lock the victims out of their device and demand bitcoins, or ask them to forward the link to two or more acquaintances. When the referrals installed the file and paid the ransom, the victim's device was unlocked.[3]

Interestingly, among those who are uncomfortable with the new threat perception, as few as 22 percent (Figure 4) feel in control of their security in a physical environment across the personal, financial and medical domains. Even fewer, 13 percent, say they feel in control of their safety in the online world.

As such, these consumers would benefit from more support to handle perceived threats across both the physical and online worlds.

Figure 4: Not in control in both online and physical worlds



Source: Ericsson ConsumerLab, Online Threats Go Offline, 2017
Base: Internet users aged 15-69, 17 countries

[2] India Today, October 2016, indiatoday.intoday.in/technology/story/32-lakh-atm-cards-hacked-is-your-debit-card-safe-should-you-change-pin-everything-you-need-to-know/1/791424.html
[3] CNBC, December 2016, www.cnbc.com/2016/12/13/popcorn-time-ransomware-hackers-ask-people-to-infect-other-computers-to-get-files-back.html

ON THE BRINK

Those who do not feel in control of their safety, although are yet to connect online activities to physical threats, comprise 35 percent of internet users surveyed. In this sense, they are uncomfortable with the traditional threat perception.

Half of this group lives in small cities, towns and villages, which is significantly above the average. Furthermore, as many as two in five of them are less frequent internet users, using internet-based services and applications on any device, less than once a day.

Figure 5 shows that only 37 percent in this group go on social networks for an hour or more a day. It's likely that as they increase their use of various online services, they will change from having a traditional threat perception to thinking that online and physical threats are interlinked.

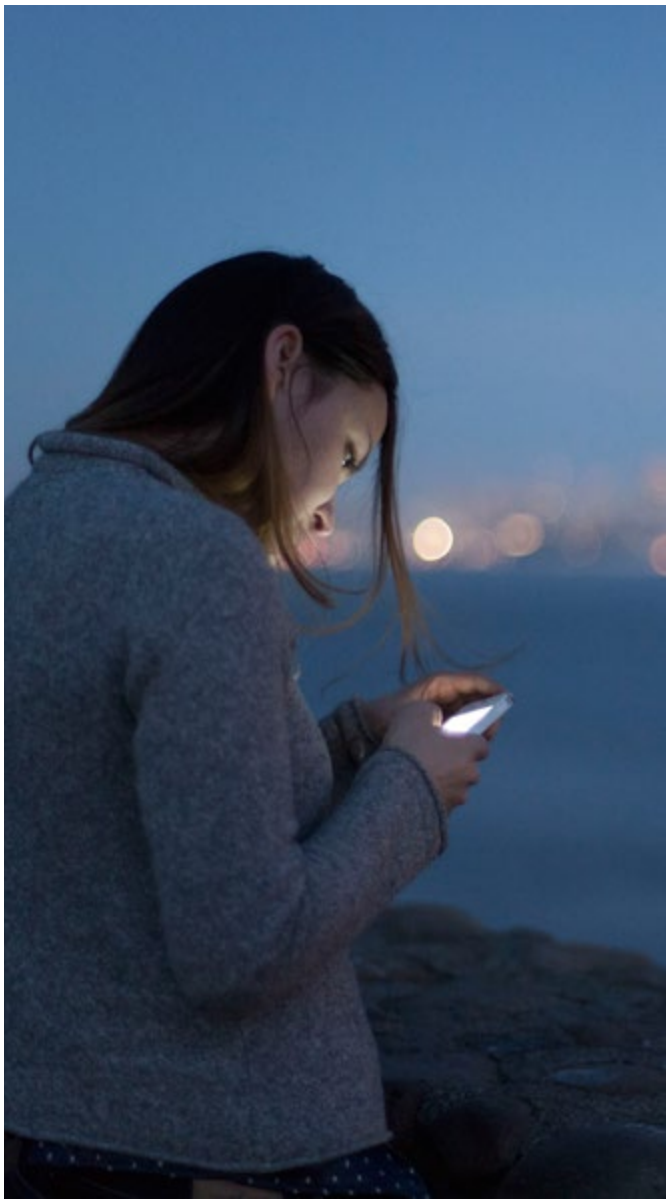
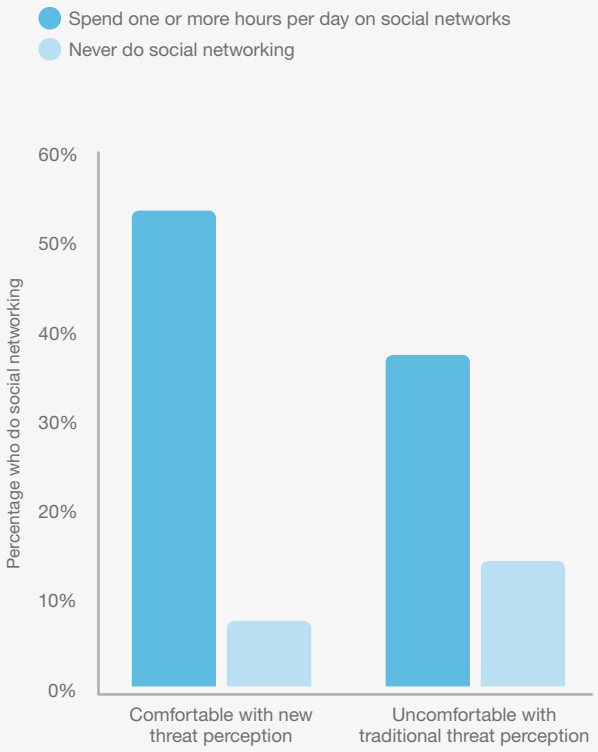


Figure 5: Spending less time on social networks



Source: Ericsson ConsumerLab, Online Threats Go Offline, 2017
Base: Internet users aged 15-69, 17 countries

Two in five of those uncomfortable with the traditional threat perception are less frequent internet users

Since these consumers are less frequent internet users, only a few of them are concerned about threats in the personal, financial and medical online domains. Although on a lower level, the key concerns among these consumers are related to their personal and financial information getting compromised or misused. For instance, one in four worries about someone using malware to hack into their system and access personal information, and a similar proportion are hesitant to share financial details for online purchases. Less than one in four is concerned about being a victim of social engineering or phishing attempts.

Going forward, it will become important to focus on what can be done to create an environment where these consumers feel safe.

ONLINE SAFEGUARDING MEASURES

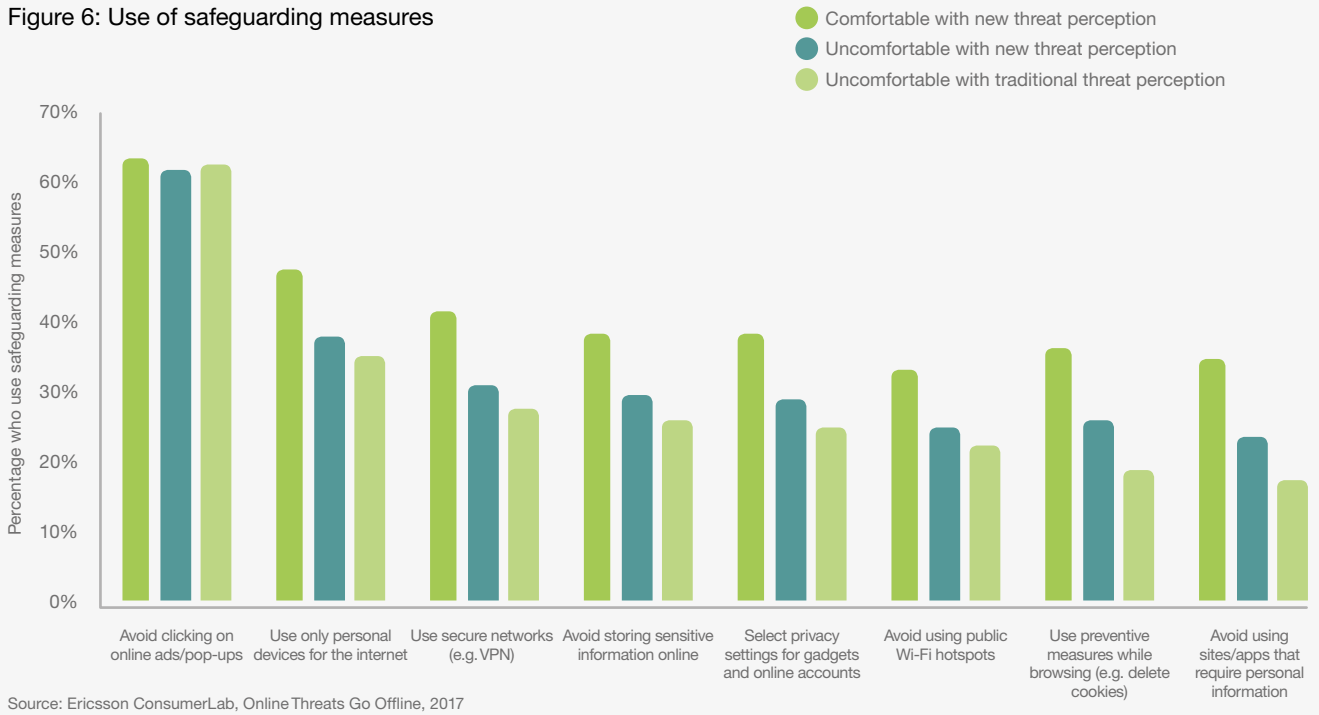
Three in five internet users do not feel in control of their safety, regardless of whether they have a new or traditional threat perception.

Those who use more safeguarding measures have the greatest feeling of safety. As seen in Figure 6, a higher proportion of consumers who are comfortable with the new threat perception, use more safeguarding measures. Additionally, half of the people in this group always use five or more online safeguarding measures; compared to one in three in the group who is uncomfortable with the traditional threat perception.

At an overall level, people seem to consciously avoid clicking on advertisements or pop-ups to prevent being unknowingly directed to a malicious website.

With the rising number of connected devices and increasing use of the internet, safeguarding against threats poses a complex challenge. For instance, 26 percent use 3 devices (smartphone, laptop or desktop, and tablet) and another 40 percent use 2 devices to go online every week.

Figure 6: Use of safeguarding measures



Source: Ericsson ConsumerLab, Online Threats Go Offline, 2017
Base: Internet users aged 15-69, 17 countries

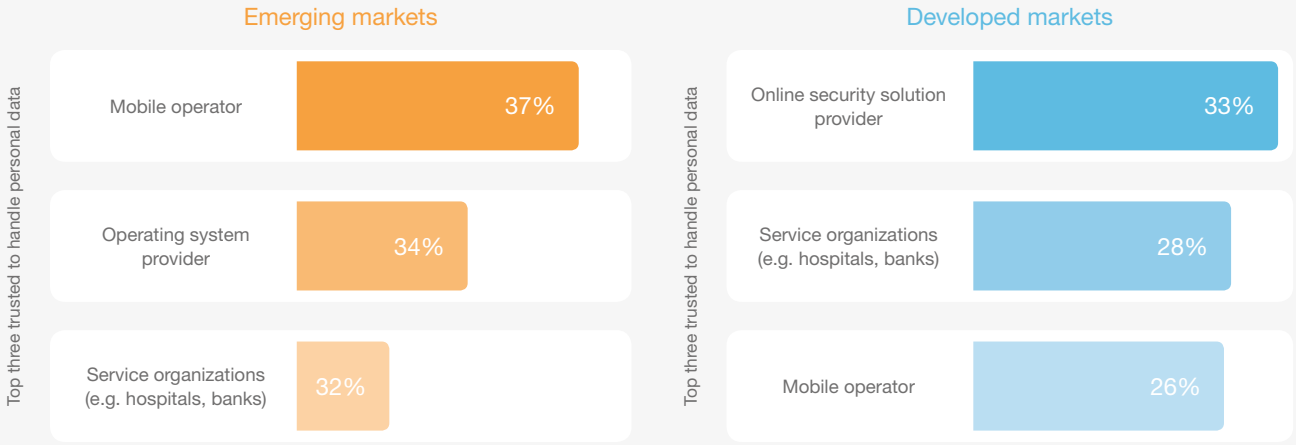
TRUSTED FOR SAFEGUARDING ONLINE

The level of control people feel in securing themselves impacts whom they trust with their personal data. Those who are comfortable with the new threat perception have higher levels of trust in organizations to safeguard their personal data, particularly when compared to the group that is uncomfortable with the traditional threat perception.

Globally, when it comes to managing personal data, 27 percent trust their own government and only about 15 percent trust foreign governments. This could be attributed to a spate of incidents in recent years where governments have been the victims of hacking, putting sensitive and confidential data at risk. For example, in the Czech Republic, many ministry officials' emails were hacked, causing a serious threat to national security.[4]

It was found that a higher percentage of internet users in developed markets trust online security solution providers to handle their personal data, whereas a higher percentage in emerging markets trust mobile operators the most (Figure 7).

Figure 7: Those trusted by consumers differs



Source: Ericsson ConsumerLab, Online Threats Go Offline, 2017
Base: Internet users aged 15-69, 17 countries

A higher percentage of internet users in developed markets trust online security solution providers to handle their personal data, whereas a higher percentage in emerging markets trust mobile operators the most

This pattern is evident across all groups, irrespective of whether they have a new or traditional view on threats, indicating that consumers in developed markets prefer more specialized organizations to handle their data.

Overall, the key areas in which consumers want support are in preventing online identity theft and in securing financial and contact information online. A primary concern is that their personal information is available in the public domain.

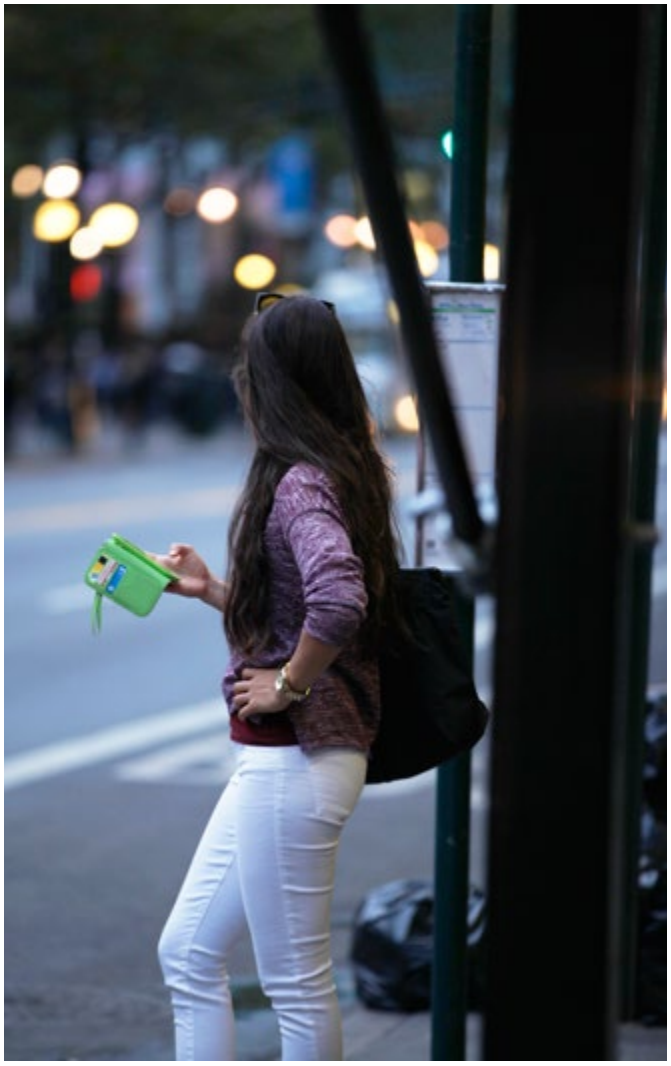
[4] Source: NY Times, 31 January, 2017, www.nytimes.com/2017/01/31/world/europe/czech-government-suspects-foreign-power-in-hacking-of-its-email.html?_r=0

STRENGTHENING THE ECOSYSTEM

Given that online threats can manifest in the physical world in so many ways, it is worrying that the systems and services for dealing with online threats do not always mirror the ones in the physical world.

Currently, various players – be it operating system providers, app or service providers, mobile operators or institutions like banks or hospitals – have limited collaboration and operate in silos to provide security solutions in their own sphere. However, the reality is that even the slightest breach in security can have a broad impact. The question is: given the scope and complexity of online threats and their impact on the physical world, can a single authority handle the responsibility of safeguarding? What about jurisdiction?

In an ecosystem where different entities provide specific services to consumers, all these organizations need to play their part in securing the environment.



Mobile operators' unique market position

Today, mobile operators are often expected to provide customer data to law enforcement agencies when required; for instance, three of the four operators in the UK were providing customer call records to police forces in 2014 through an automated system.[5] That said, they may also be in a unique position to directly help consumers due to their presence online, in brick and mortar stores and on 24/7 helplines. Compared to operating system providers, app service providers and others who usually have limited consumer interactions across these touch points, mobile operators have an ongoing engagement with their customers.

Given that mobile operators can provide localized support at their customers' location, which others cannot, they could potentially offer immediate assistance in an event where a threat makes its way from the online to the physical world.

This role could include multiple aspects such as providing certifications for the device, ensuring a secure experience – or tie-ups with various service and app providers – to help guide consumers to services that have been accredited and deemed secure. This could be particularly relevant in emerging markets, where internet users already trust mobile operators more than other players to handle their personal data.

Mobile operators may be in a unique position due to their presence online, in brick and mortar stores and on 24/7 helplines

[5] The Guardian, October 2014, www.theguardian.com/world/2014/oct/10/automatic-police-access-customers-mobile-phone-records-like-cash-machine-ripa-three-ee-vodafone

PRIMING FOR A NEW REALITY

So what does the future look like? Automated homes, smart appliances and augmented realities are all expected to become mainstream in the near future.

Analysis across 21 countries found that 46 percent of internet users would like help with activities such as managing day-to-day activities, housework, meal planning and shopping. Furthermore, 84 percent of those who want support would like fully automated products, tools or apps to do the work for them.

When such connected and advanced technologies become mainstream, they will bring new challenges in a world where online and physical threats are already interlinked. Is hacking connected home systems a way to break into homes? Is hacking into an autonomous car the new face of carjacking? The lines between actions in the online and physical worlds are set to become even more blurred. Secure networks and protected passwords will need to be supplemented with more evolved safeguarding measures.

Looking at the consumer groups described in this report, it becomes evident that future solutions will not be just about creating a safe and risk free environment – a place with no sharp corners. Given that the group most comfortable with the new threat perception already mixes and matches a plethora of safeguarding measures, these solutions must become increasingly easy to adapt and personalize, allowing people to continue to take risks online while remaining comfortable with how to handle such risks. The internet is built on interaction and constant change – and security solutions must behave similarly, or risk being perceived as limiting straitjackets.

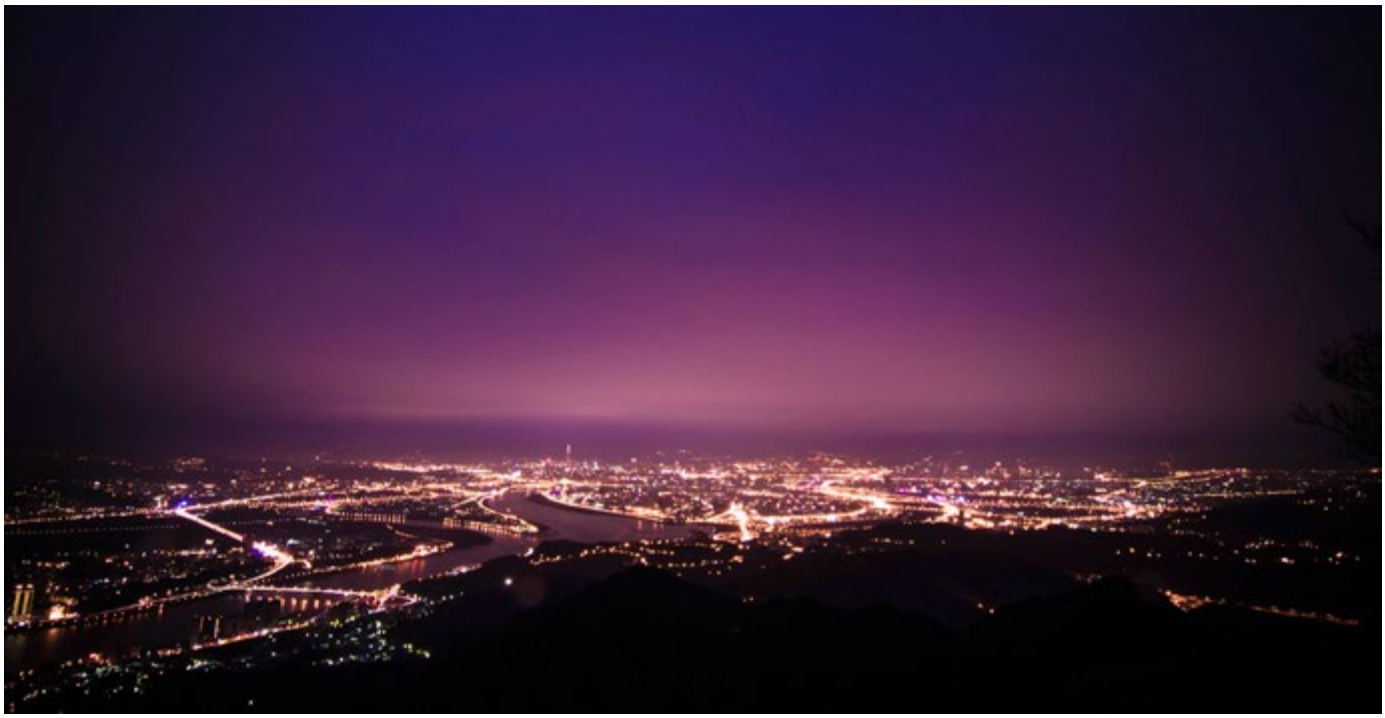
Security solution providers need to take into consideration that threats will cross the online and physical domains

At the same time, more security solution providers need to take into consideration that threats will cross the online and physical domains; for instance, security providers should be able to identify, support or advise if online stalking becomes a physical threat. Such support needs to be personalized so that a user can create alerts for different types of personal data, such as location information or heartrate readings being accessed by an unauthorized user.

In other words, needs for safeguarding against a wide range of online and physical threats will vary for different users – and they will also want to employ safeguarding measures differently.

Younger generations, who have grown up with flexible platforms such as YouTube and Minecraft, will expect to be able to alter services and share security mods without hampering the experience – just as they can alter and modify their media and gaming environments at will today.

As the internet continues to evolve and become even more interactive and ever-present in daily life, our expectations on security solutions will also advance.



Ericsson is a world leader in communications technology and services with headquarters in Stockholm, Sweden. Our organization consists of more than 111,000 experts who have provided customers in 180 countries with innovative solutions and services. Together we are building a more connected future where anyone and any industry is empowered to reach their full potential. Net sales in 2016 were SEK 222.6 billion (USD 24.5 billion). Ericsson is listed on NASDAQ OMX stock exchange in Stockholm and the NASDAQ in New York.

Read more on www.ericsson.com

Ericsson
SE-Stockholm, Sweden
Telephone +46 10 719 0000
www.ericsson.com

GFSA-17:000043 Uen