White Paper

Bitdefender®

Security Awareness in the Age of Internet of Things

A 2016 Bitdefender Study

Summary

A talking kettle? A fridge that orders groceries while you're at work? Plants that water themselves? 6.4 billion of these futuristic gadgets[1] already occupy a privileged place in people's homes, whether it's wireless sensors, network-connected webcams, smart plugs and Wi-Fi enabled light bulbs that turn baby blue when users receive a new Facebook message.

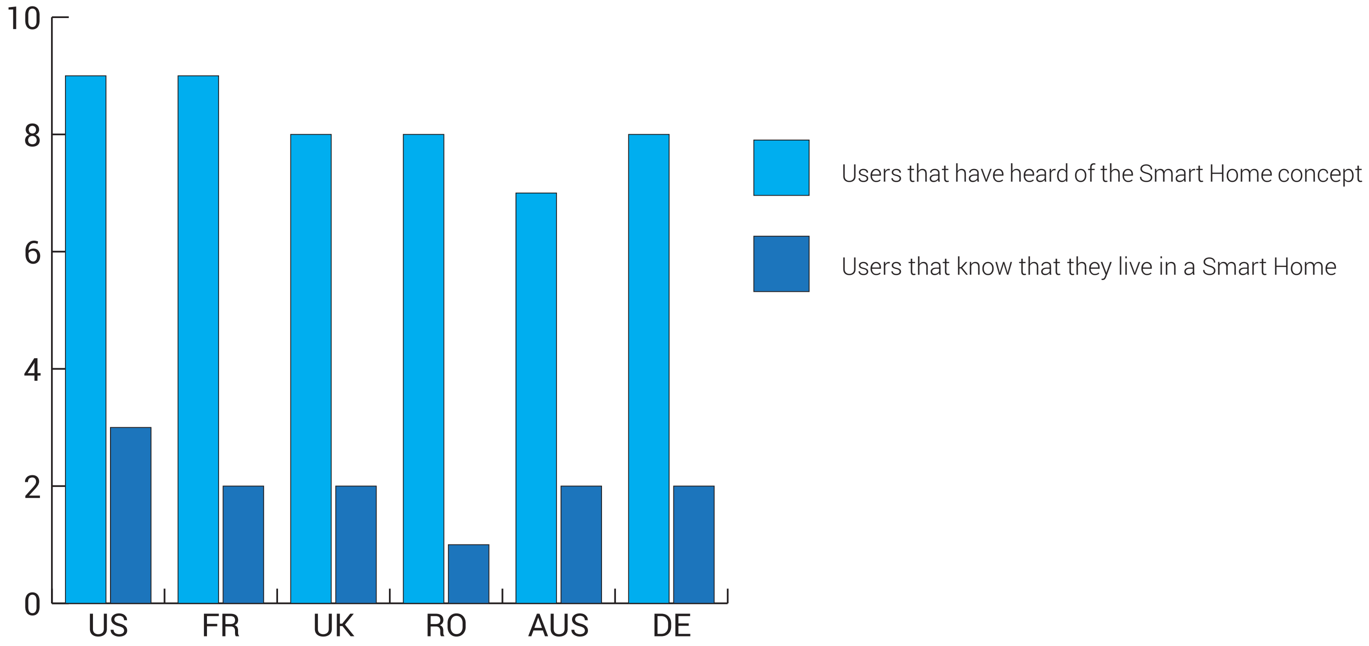
The "Jetsonian" home is already here, thriving before our eyes. But are people aware of it?

This paper looks to shed light on home users' perception of smart technologies, to showcase how consumer IoT is embraced and understood by Internet users around the United States and Europe. Without a doubt, people are excited by the novelty of connected objects, but how well do they manage security and privacy? Are they succeeding or failing as the administrator of Things in their homes?

Key Findings

More users have heard about smart homes than about the Internet of Things. A fifth or less realize they live in one.

Tests on the notoriety of two key concepts, "The Internet of Things" and "Smart Home" reveal confusion among users and dilution of the two terms. **Half of Internet-connected users based in the US have not heard of the concept of "Internet of Things," the study suggests.**



American and French users seem more informed than others. In both countries, 9 out of 10 technology users have heard of the Smart Home concept. In the US, 5 out of 10 have heard of the Internet of Things concept, while in France 6 out of 10 know about it. Of users who technically live in a connected home, only 3 out of 10 US users are aware of it, while in France 2 out of 10 (17%) know they live in a smart home.

In the UK, 8 out of 10 users have heard of the Smart Home concept, while 5 out of 10 use the term "IoT". Only 2 out of 10 smart home users realize they live in one.

The same awareness level appears to be among Romanian users. 8 out of 10 technology users have heard of the Smart Home concept, while significantly fewer (4 out of 10) have an idea about what IoT is. When asked, only 1 out of 10 smart home residents know they live in one.

In Australia, 7 out of 10 technology users have heard of the Smart Home concept, as opposed to 5 out of 10 users who are aware of the Internet of Things. Only 2 out of 10 smart home users know that they live in one.

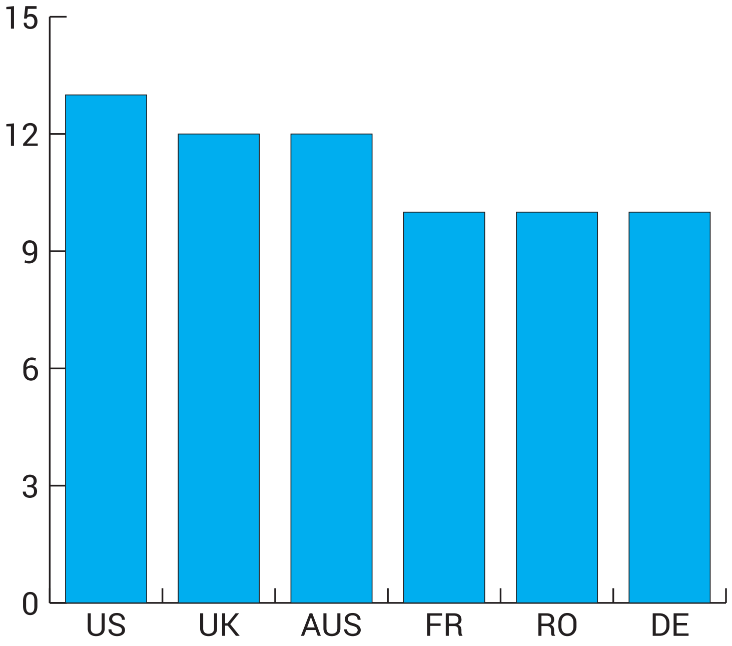
[1] http://www.gartner.com/newsroom/id/3165317

When asked about the concepts of IoT and Smart Home, 9 out of 10 German Internet users said they heard about the latter, yet only 2 out of 10 know they are living in one.

Smart devices ownership

On average, a household from the United States carries 13 smart devices or accessories. There are 12 in the UK and Australia, and 10 in France, Romania and Germany.

Smart gadgets per household



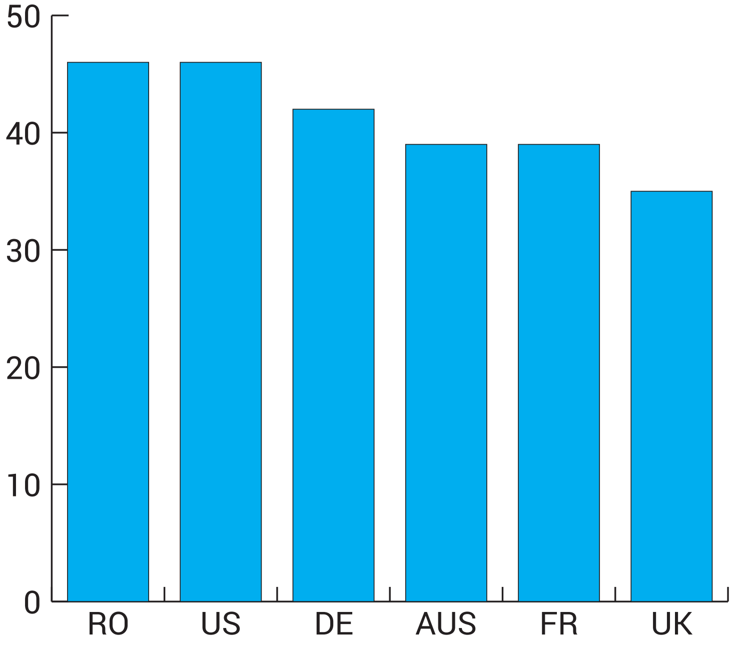
When asked about Internet connectivity, most IoT users said they have a clear overview of how many of the smart devices in their homes are connected to the Internet.

In most homes, the top devices that have access to the home's Wi-Fi network are smartphones, Windows desktop computers and tablets, followed by smart TVs and wireless gaming consoles.

Biggest security concerns

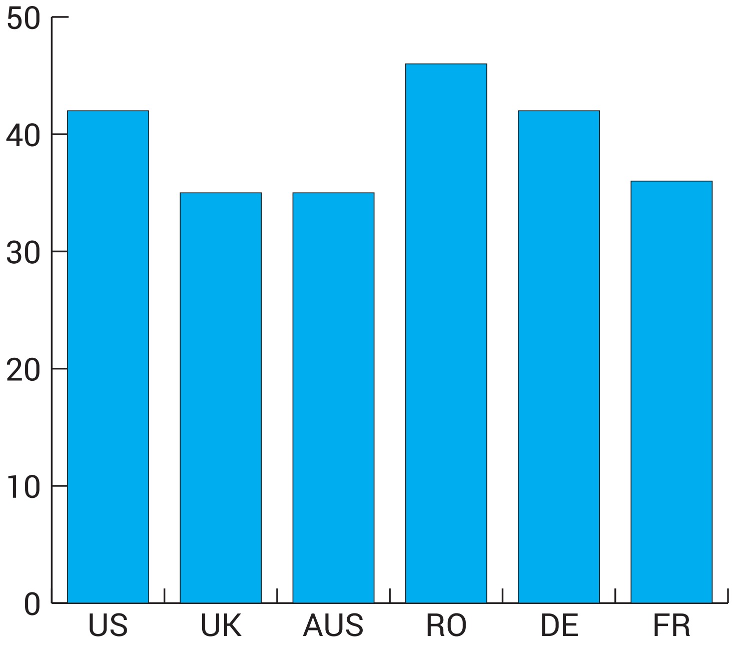
One roadblock to large-scale IoT adoption is security. Most technology users are concerned that personal information can be stolen or leaked through intelligent gadgets (46% in the US and Romania, 43% in Germany, 39% in Australia and France, 35% in the UK).

Top privacy concerns



Secondly, users fear that someone can take control of their devices over the Internet (42% in the US, 35% in the UK and Australia, 35% of Romanian users, 45% in Germany, 36% in France).

Losing control of smart devices



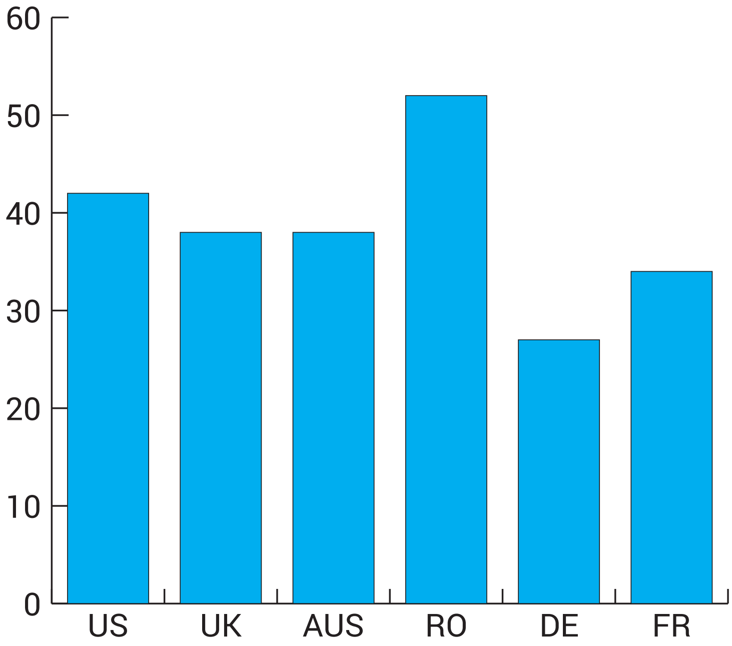
Their concerns are amplified by studies that showcase the dangers of an insecure device in a home. Recently, Bitdefender researchers[2] discovered that a smart webcam could be hijacked and turned into a full-fledged spying tool. Anyone taking advantage of poor server authentication could register to the manufacturer's servers and pose as the original device, to take full control of it. This could result in spying on people's families and even talking to children who had the monitoring devices in their rooms.

"More people need to realize that attackers are not targeting only the device," says Alexandru Balan, Chief Security Researcher at Bitdefender. "They look for an easy entry point into your home network, to see how they can break into other connected machines and steal any unsecured information passing through the network."

Unless communication is encrypted against interception and tampering, cyber-criminals can perform a man-in-the-middle attack and pilfer data sent between application, device and server. If they get full access, they can also falsify information, crash the device or enlist it in a DDoS attack against online targets without the user's knowledge.

When asked about the possibility of device theft, Australians and Romanians put this at the top of their list of concerns. 42% of Australians cite this as their number one fear. 39% of Romanians, 37% of US users, 33% of UK users, 30% of French users and 25% of German users feel the same.

Fear of getting robbed



Security advice to prevent prying eyes

To stop rogue users from intercepting communications, privacy-minded users should enhance network security by strengthening credentials, enabling network encryption and keeping device firmware up-to-date. A dedicated IoT security solution[3] is also key for sanitizing traffic and blocking any man-in-the-middle attempts.

[2] https://labs.bitdefender.com/2016/11/smart-webcam-can-go-rogue-to-spy-on-kids-bitdefender-finds/
[3] http://www.bitdefender.com/box/

The importance of updates

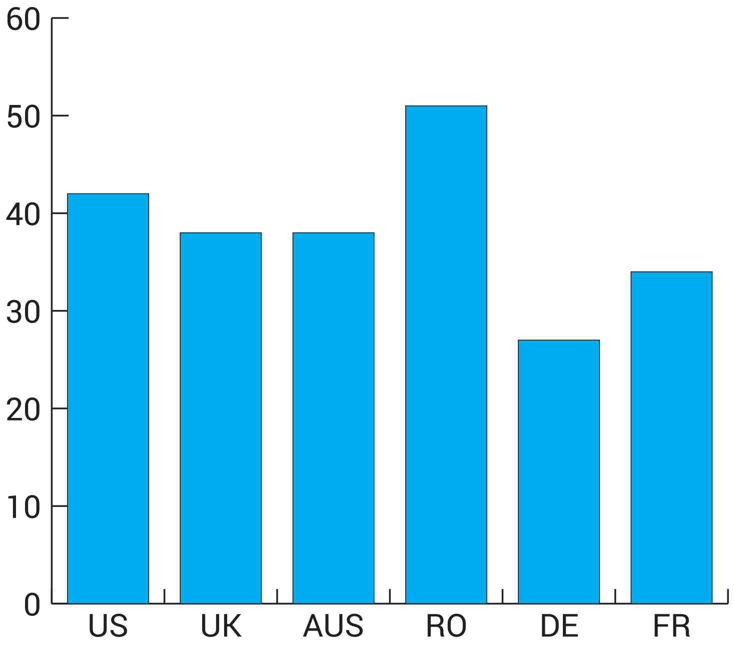
Smart TVs are among the most popular Internet-connected devices. In 2017, 244 million units are expected to be delivered globally, according to statistics.[4] And it's no surprise, as Internet-ready TVs come with built-in capabilities to access streaming media services, run entertainment apps and navigate web browsers.

In the US and UK, 23% of Smart TV owners use their device to browse the internet and 38% of Romanian users do the same, as well as 26% of Australians, 24% of Germans and 17% of French users.

However, **most users neglect software updates.**

42% Americans have never updated the firmware or default software package. A similar situation regarding performing updates can be found among Romanians (51%), Brits and Australians (38%), Germans (27%) and French users (34%).

Frequency of software updates



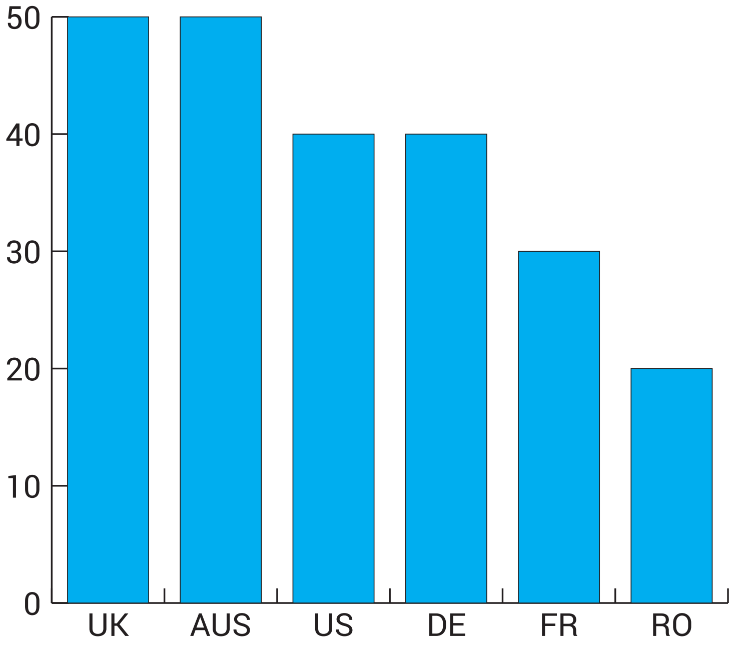
The main reason cited by most users is the lack of knowledge, as 4 out of 10 US users admitted, followed by the lack of time and fear of crushing the system.

Automatic updates usually take a few clicks, several minutes and minimum tech skills, however, manual updates also require a computer and USB drive. To manually update smart TV software/firmware, the user needs to go to the manufacturer's download page, choose the latest firmware release and click to download the upgrade file on a Windows computer. Then, transfer the executable to a USB stick and insert it in the TV's slot.

The absence of expertise is cited by more than half of UK users and Australian respondents, 4 out of 10 US-based and German users and 2 out of 10 Romanian users. 3 out of 10 French users that did not update the Smart TV's software say they didn't have time, or think software updates aren't helpful.

[4] https://www.statista.com/statistics/314616/smart-tv-unit-shipment-worldwide-forecast/

Reasons for not updating (lack of knowledge)



Security advice for smart TV owners

After purchasing a smart TV, Bitdefender advises users to enhance their privacy and:

- Secure their wireless routers with strong, unique passwords.
- Isolate the Internet-connected TV on a separate network, if possible.
- Install only authorized apps provided by the manufacturer.
- Use strong passwords for all Internet accounts (Netflix, Facebook, Skype etc.)
- If the TV has a built-in camera, pause it when not in use.
- Avoid any unexpected messages appearing on your TV screen requesting permission to link a device or enable a remote session.
- Use a dedicated home security solution to stop malware, phishing attempts and rogue users.

Password habits

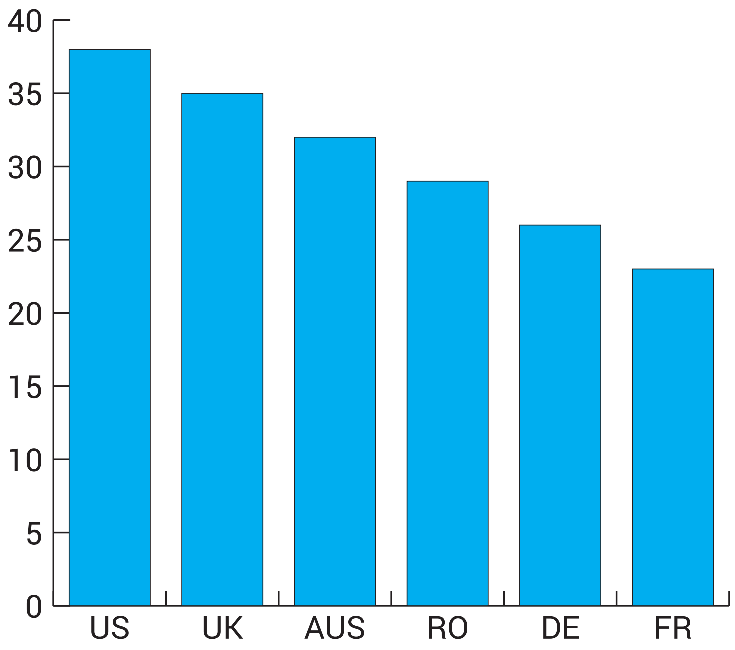
5 out of 10 of smart TV owners in the UK, Australia, Germany and France said they have never changed the password on their device. Similarly, 4 out of 10 Romanian and US users said that they have never changed it.

Other devices are equally neglected. For instance, 4 out of 10 US users claim that they have never changed the password for their smartphones and tablets.

More worrisome is the fact that **16% of US users use the same password for all devices.** However, 45% of US users say they have a different password for each device. French and German users set a better example, with more than half (57% and 56%, respectively) claiming to secure each device with a unique password, followed by UK users (47%), Australians (46%) and Romanians (43%).

When it comes to reusing passwords, roughly a third of users say they have a set of passwords which they rotate between accounts - namely 38% of US users, 35% UK users, 29% of Romanian users, 23% of French users, 26% of Germans, and 32% of Australians.

The perils of alternating passwords



Password reuse is the root cause of some of the worst security breaches to date. A hacker got into Dropbox because an employee who was using the same password for his LinkedIn account, which was previously leaked. The hacker gained access to Dropbox's corporate network, where 68 million user credentials were stored.

Despite this, IoT devices are often pushed to market without strong authentication security mechanisms. Publicly leaked data reveals that smart devices are secured with basic, default passwords like "1234" or require no passwords at all. Consequently, brute-force attacks are often successful at dismantling them and help attackers get easy access to the device and the user's network.

"Almost every gadget we've analyzed in our ongoing security research on IoT gadgets displayed weak user credentials and no hotspot authentication," says Alexandru Balan, Chief Security Researcher at Bitdefender. "Changing default passwords is a critical security practice, yet a lot of users still ignore it".

Security tips for protecting accounts

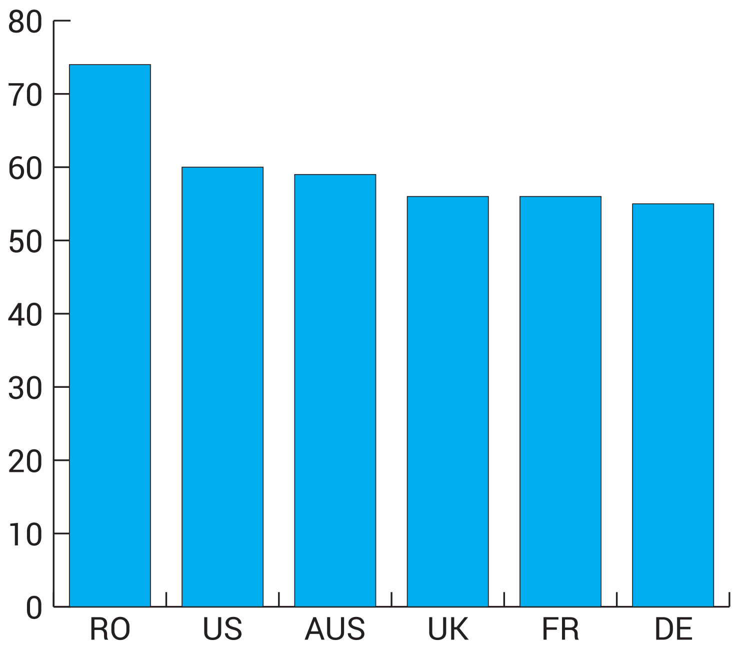
Users should never forget to assign unique, complex passwords for their accounts and devices, regardless if they receive reminders from manufacturers or not. Applying an extra layer of protection, where possible, via two-factor authentication methods, is also key in significantly reducing the risk of account breaches.

Data loss prevention

The biggest security risks revolving around IoT are related to losing private information, such as account passwords and email addresses, network passwords, images or banking information. That's why backup is essential. We asked users how they store and safeguard their most precious belongings, and this is what we found out.

In the US, 60% of users keep private photos and documents on personal laptops, a number only surpassed by Romanians, with 74%. Other countries follow with similar percentages: 56% of UK users, 59% of Australians, 56% of French users, and 55% of German users.

Well-liked backup solutions



"Keeping important, personal data on devices connected to the Internet increases the odds of getting infected with ransomware, for instance," Balan says.

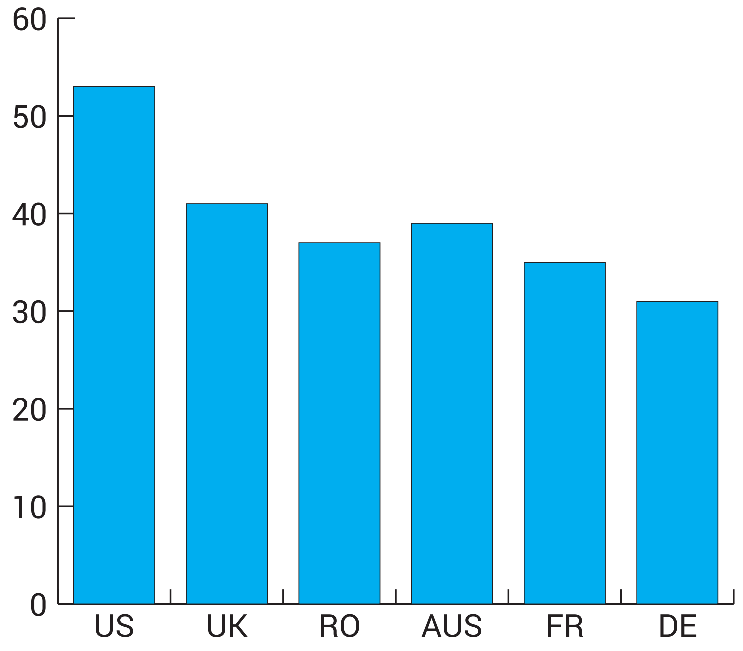
Almost 13 million people have been targeted by ransomware in the US alone, however, 32% of users unaffected by ransomware think it is improbable or very improbable they will get infected, according to a Bitdefender study[5] on ransomware victims.

Another favorite backup solution remains hardware. 47% of US users keep private files on physical devices such as USB storage or DVDs. This number is similar to its European counterparts - 46% of UK users. 55% of Australians, and 50% of German users. French users (62%) choose this one as their preferred tool, only surpassed by Romanians (73%).

Cloud storage solutions are second best for Americans after personal PCs, as 53% opt for it, together with 41% of UK users, 37% of Romanian users, 39% of Australians, 35% of French users and 31% of Germans.

[5] http://download.bitdefender.com/resources/files/News/CaseStudies/study/59/Bitdefender-Ransomware-A-Victim-Perspective.pdf

Trusting the cloud



Other storage options include smartphones, which come fourth on the list of options for users in most countries, except Romania, where they rank 3rd (42%) and Germany, where they are fourth, with 19% of users.

Interestingly, in the US, a third of IoT-aware users keep their private data on office laptops, a practice known to bear legal implications, unless company policies clearly address ownership, custody and access rights of the information involved.

Security tips to prevent data loss incidents

One of the most efficient backup practices is keeping copies of valuable data on an Internet-isolated hard drive. Cloud storage solutions are also an option worth considering, as long as secure cloud ecosystems protect the confidentiality, availability and integrity of the data residing in the cloud. In 2017, an estimated 1.8 billion people worldwide will be using personal cloud storage.[6]

[6] https://www.statista.com/statistics/499558/worldwide-personal-cloud-storage-users/

Conclusions

The concept of IoT is still unclear to most users, as most people relate to the concept of “Smart Home.” The biggest risks perceived by users are losing private data through improperly secured IoT devices, followed by losing access to the device itself and having the gadget stolen.

When it comes to security hygiene, old habits die hard or, better said, creating healthier habits such as updating software regularly to patch vulnerabilities or changing passwords frequently, are still difficult to form and adhere to.

“Although manufacturers are not always quick to push security updates for known vulnerabilities, users shouldn’t postpone installing them, once available,” says Alexandru Balan, Chief Security Researcher at Bitdefender. “Cybercriminals often infiltrate home and corporate networks through outdated software – so, whether it is a laptop or a smart device, security updates should be installed with the same diligence by users.”

How to enhance security

Before purchasing any Internet-ready device, users should understand exactly how a gadget works - how does it connect to the Internet, what data can it access, where is that data stored and under what circumstances? Thorough online research into the new device will help users balance the risks and benefits – can this device turn into a privacy hazard? Using data collected from it, could someone infiltrate the home Wi-Fi network to snoop on private conversations and steal other personal information?

Read privacy statements and any information regarding how data is processed. This step is sometimes overlooked by users, but may reveal surprising facts. Personal information can be shared with third parties, such as advertising companies, that will use it to create and spam users with targeted ads.

Change default passwords. Passwords are still the Achilles’ heel of security, the root of severe security breaches that have affected multi-million-dollar companies. By default, devices come with simple, yet easy-to-crack credentials that need to be replaced with unique, complex passwords.

Stay up to date on the number of devices within the household - how they operate, their security stance, who uses them, if the software is updated regularly by the manufacturer and, very importantly, if and how often they get attacked.

“Administering intelligent devices within the household is a full-time job that requires energy and a new set of skills that need to be learned,” Balan says. “All in all, as more devices hit and are the market, we expect the level of awareness and proficiency in mastering IoT security to increase as well.”

Enhance router security and use a dedicated security solution. If attackers get full access to a router, they can monitor, redirect, block or tamper with traffic and sensitive communications passing through the network. Apart from changing passwords, keeping firmware updated and turning on WPA2 encryption, users should add a strong layer of security.

Bitdefender BOX[7] is the first integrated home cyber-security solution for connected devices. Intercepting attacks at their core, the home network, Bitdefender BOX provides advanced malware and anti-phishing protection for all connected devices - smartphones, PCs, Macs, home appliances, wearables and others. The Vulnerability Assessment feature scans devices to pinpoint their security weaknesses, Active Threat Control stops never-before-seen malware, while the Private Line feature secures connections even when outside the home perimeter.

The Bitdefender IoT Awareness and Security Study was conducted in August 2016, on a sample of 2037 users from the US, the United Kingdom, Romania, Australia, France and Germany.

Author: Alexandra Gheorghe, Security Specialist at Bitdefender, November 2016

[7] http://www.bitdefender.com/box/

Bitdefender is a global security technology company that delivers solutions in more than 100 countries through a network of value-added alliances, distributors and reseller partners. Since 2001, Bitdefender has consistently produced award-winning business and consumer security technology, and is a leading security provider in virtualization and cloud technologies. Through R&D, alliances and partnership teams, Bitdefender has elevated the highest standards of security excellence in both its number-one-ranked technology and its strategic alliances with the world's leading virtualization and cloud technology providers. More information is available at
http://www.bitdefender.com/

FOR MORE INFORMATION VISIT: enterprise.bitdefender.com