

RUBIN

SCIENCE MAGAZINE

SPECIAL ISSUE

IT SECURITY

Three tough nuts for quantum computers to crack

This is how artificially generated images reveal their true colours

Start-up: Ready for the new generation of mobile communications

HOW SAFE DO PEOPLE AROUND THE WORLD FEEL ON THE INTERNET?

Who has ever been hit by cybercrime? How do people protect themselves from it? A survey reveals similarities and differences between different groups around the world.

When it comes to the internet, “evil is everywhere under the sun”, as the popular quote goes. By adopting safe practices, however, we can make it more difficult for cybercriminals to steal our data or cause damage in other ways. But what constitutes safe practices? What do you have to do to protect yourself from data theft and similar crimes? “There’s a lot of confusion about this, among people from all over the world,” is what Franziska Herbert has learned. The psychology graduate is currently completing her dissertation in the CASA Cluster of Excellence at the Horst Görtz Institute for IT Security. In collaboration with Professor Markus Dürmuth, Professor Angela Sasse and other researchers, she has conducted a comprehensive survey that assesses the human factor in IT security.

More than 12,000 individuals in twelve countries took part in the online survey, which focused on what people understand safe behaviour in cyberspace to be, how they approach it and what misconceptions they may have. Participants came from China, Germany, the UK, India, Israel, Italy, Mexico, Poland, Saudi Arabia, Sweden, the USA and South Africa. They represent 42 per cent of the world’s population. The questions revolved, for example, around end-to-end encryption, WiFi surfing, the https standard, virtual private networks (VPN), and passwords. “It emerged that some risks are equally well understood by all participants around the world,” points out Franziska Herbert, who designed the survey together with the team. One of these is the phenomenon of shoulder surfing, where unauthorised persons obtain personal data simply by looking over a user’s shoulder.

Certain misconceptions, however, are apparently also widespread around the world. “For example, in all the countries we covered in the survey, 80 per cent of the participants believe that it is necessary to change passwords periodically to keep them secure,” says Franziska Herbert. IT security experts actually used to recommend this for a long time, until it

turned out that this practice actually doesn’t do any good at all. “All that happens is that passwords become more and more insecure as a result, because otherwise users won’t be able to remember them. It’s much better to choose really strong passwords that are not easy to crack – a password manager is very helpful for this purpose,” explains Franziska Herbert. “Once you have a secure password, you can stick to it, as long as it doesn’t fall into the wrong hands.”

Participants in all countries also agreed with the statement that their computers could be infected by malware when they click on a link. “This only happens in a few exceptional cases,” say the researchers. “Most of the time, further actions are needed, such as entering data on the website accessed via the link.”

The researchers also found that uncertainty about IT security issues prevailed across the board among participants worldwide. “This is reflected in the fact that our survey participants chose exactly the middle on a scale ranging from ‘completely agree’ to ‘completely disagree’ on many questions,” says the researcher.

In addition to all the similarities, the researchers also identified differences between participants from different countries, especially with regard to the scale of the assessments. “We found the biggest differences to exist between Western and non-Western countries,” says Herbert. The researchers include China, India, Mexico, Saudi Arabia and South Africa among the latter. “Compared to participants from Germany, participants in all other countries were more likely to have misconceptions about malware, device security and passwords,” outlines Franziska Herbert. German participants were the least likely to agree with misconceptions – even though they still fell in the middle of the scale between ‘completely agree’ and ‘completely disagree’. The highest level of agreement with misleading statements came from participants from China and India.



In public, a glance over the shoulder is enough to spy out passwords, for example.



OF THE PARTICIPANTS BELIEVE THAT IT IS NECESSARY TO CHANGE PASSWORDS PERIODICALLY TO KEEP THEM SECURE.

Two examples from the survey:

“I am more likely to catch malware when I visit a porn site than when I visit a sports site.” Approximately 49 per cent of respondents in Germany agreed with this misconception, while 75 per cent from Saudi Arabia and 86 per cent from China agreed with it.

The correct statement “Links in emails can lead me to fake websites in order to intercept my login data” was agreed to by 87 per cent of German participants and 78 per cent of Chinese participants.

All groups participating in the survey had in common that they tended not to consider family and friends an IT security risk. “That’s not how we see it,” says Markus Dürmuth. There are risks, especially when people share a computer or passwords. When it comes to domestic violence or stalking, it’s often people in a user’s closest circle who pose a threat. “And there’s another thing: among friends, pranks may be played that are not at all funny for the victim,” concludes the researcher.

text: md, photos: ms



Franziska Herbert wants to know how safe people feel on the internet and what experiences they have had.

EDITOR'S DEADLINE

The rabbits in the CASA Universe are startled: the seemingly well-secured access to Rabbit Mark's carrot stash has been hacked and all winter supplies have been stolen. The brave bunny Betty then starts looking for support at the nearby CASA Hub C – a mysterious place that is supposed to hold solutions for digital security. Thus begins the adventure of Betty the bunny, the protagonist of the first science comic from the Cluster of Excellence CASA. Along with Betty, the readers explore the Research Hub and learn about the research priorities and challenges that the scientists in the Research Hub C "Secure Systems" deal with on a daily basis. Find out how to read this and more CASA comics at no cost at:

➔ casa.rub.de/en/outreach/science-comics



Answers
DEEP FAKE-QUIZ
The following faces
are real:
1a, 2a, 3b, 4a, 5b, 6a

??

LEGAL NOTICE

PUBLISHER: Cluster of Excellence CASA at the Horst Görtz Institute for IT Security at Ruhr University Bochum in collaboration with the Corporate Communications Department at Ruhr University Bochum (Hubert Hundt, v.i.S.d.P.)

EDITORIAL ADDRESS: Corporate Communications Department, Editorial Office Rubin, Ruhr-Universität Bochum, 44780 Bochum, Germany, phone: +49 234 32 25228, rubin@rub.de, news.rub.de/rubin

EDITORIAL BOARD: Dr. Julia Weiler (jwe, editor-in-chief); Meike Drießen (md); Lisa Bischoff (lb)

PHOTOGRAPHER: Michael Schwettmann (ms), Dammstr. 6, 44892 Bochum, Tel.: +49 177 3443543, info@michaelschwettmann.de, www.michaelschwettmann.de

COVER: Sashkin – stock.adobe.com

PHOTOGRAPHS FOR TABLE OF CONTENTS: Michael Schwettmann

GRAPHIC DESIGN, ILLUSTRATION, LAYOUT:
Agentur für Markenkommunikation, Ruhr-Universität Bochum,
www.einrichtungen.rub.de/de/agentur-fuer-markenkommunikation

PRINTED BY: LD Medienhaus GmbH & Co. KG, Van-Delden-Str. 6-8, 48683 Ahaus, Germany, Tel.: +49 231 90592000, info@ld-medienhaus.de, www.ld-medienhaus.de

EDITION: 800

DISTRIBUTION: Rubin is published twice a year in German language; the regular issues are available from the Corporate Communications Department at Ruhr-Universität Bochum. The magazine can be subscribed to free of charge at news.rub.de/rubin/abo. The subscription can be cancelled by email to rubin@rub.de. The special issue 2021 is available from the Horst Görtz Institute for IT Security. In case of interest, please contact hgi-presse@rub.de.

ISSN: 0942-6639

Reprinting with reference to source and submission of proof copies