

Want to Raise Cybersecurity Awareness? Start with Future IT Professionals.

Lydia Kraus, Valdemar Švábenský, Martin Horák, Vashek Matyáš, **Jan Vykopal**, Pavel Čeleda
vykopal@fi.muni.cz

Masaryk University, Czech Republic

July 10, 2023, ACM Conference on Innovation and Technology in Computer Science Education (ITICSE), Turku, Finland

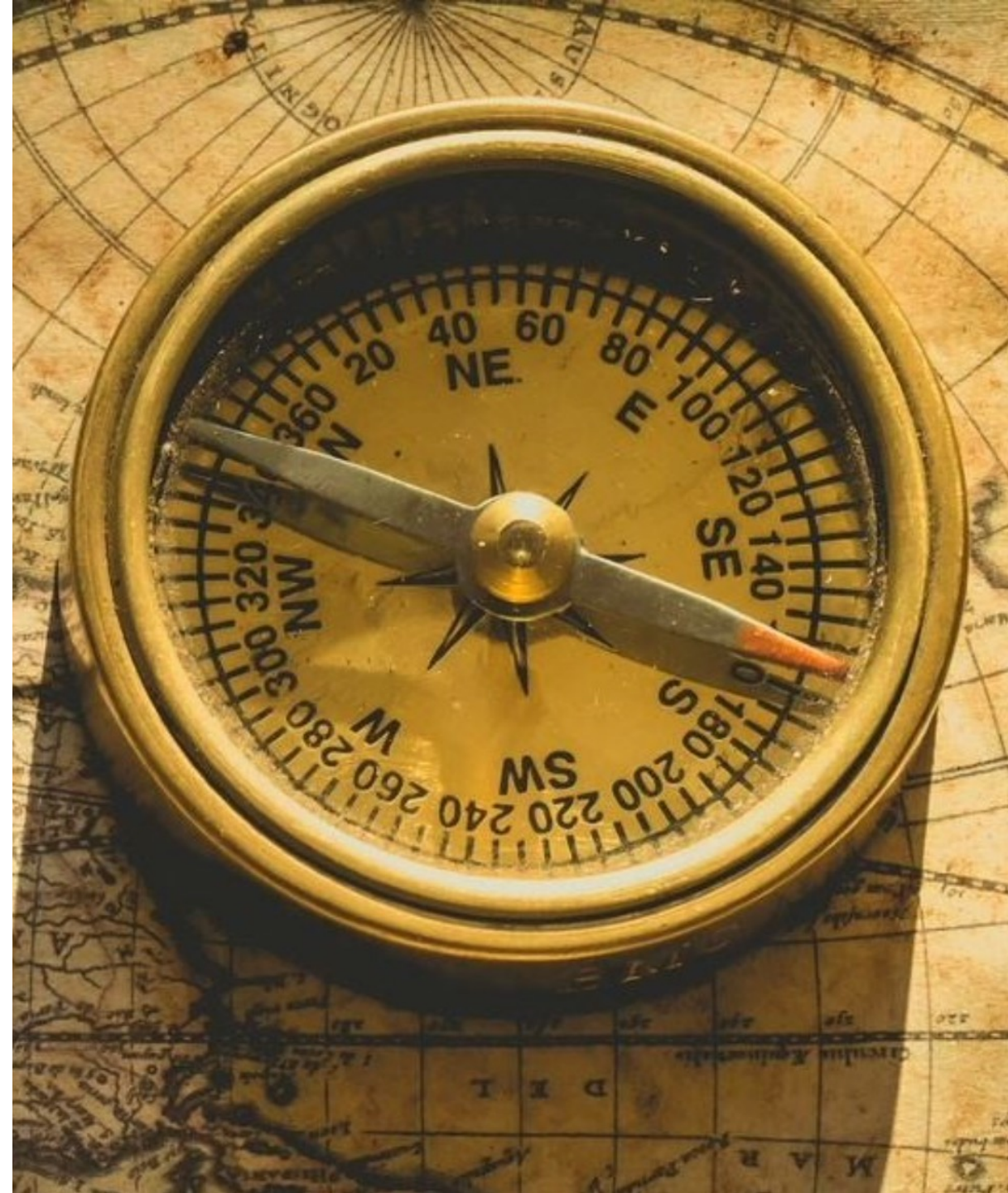
Motivation

- A public university with **various faculties** and departments.
- About **33,000 students** at 10 faculties, **6,500 employees**.
- More than **1,000 cybersecurity incidents every year**.
- Many can be **prevented by efficient education of end users**.



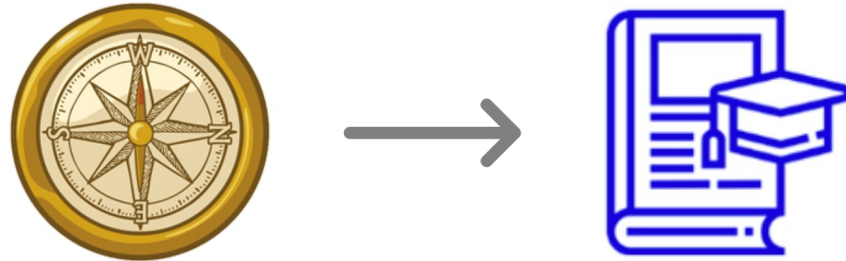
Solution: Cybercompass

- *The navigator to the golden middle way in the world of cybersecurity.*
- Aims to **raise awareness** about essential **cybersecurity topics**.
- Helps users to **implement** basic defensive **countermeasures**.
- **Online** course, extracurricular activity.
- **Freely** available resource for students, employees, and the public:
<https://security.muni.cz/en/cybercompass>



Paper goal

Evaluation of the effects of including cybersecurity awareness course into an introductory security course.



Cybercompass lessons



Security of devices



Passwords



Cybersecurity self-defense



Secure communication



Incident reporting

Cybercompass: Lesson structure

Each lesson:

- text with information on cybersecurity threats
- tutorials of protective tools (e.g. antivirus, password manager)
- takes 15-30 minutes to complete

What's the lesson about?

Copying the entire hard disk content within ten minutes, without you even noticing it. Retrieving data from a turned-off smartphone via a USB cable – and using them against you. Losing private pictures because of an unsecured device. We're not exaggerating; this is the reality. You may accept it either in the form of preventive measures or consequences.

In this lesson, you'll find handy tricks for the security of smartphones, which is often overlooked. Nevertheless, the recommendations apply for mobile devices (laptops, tablets) and PCs as well. Are you scared of words like authentication, encryption, or data backups? Sounds like a job only for "the IT people"? We will show you that you can best protect your data and devices by yourself, and that most precautions will take like five clicks. Get ready, prepare all your devices; we are going secure!



EXTRA 20 MIN



7 CHALLENGES



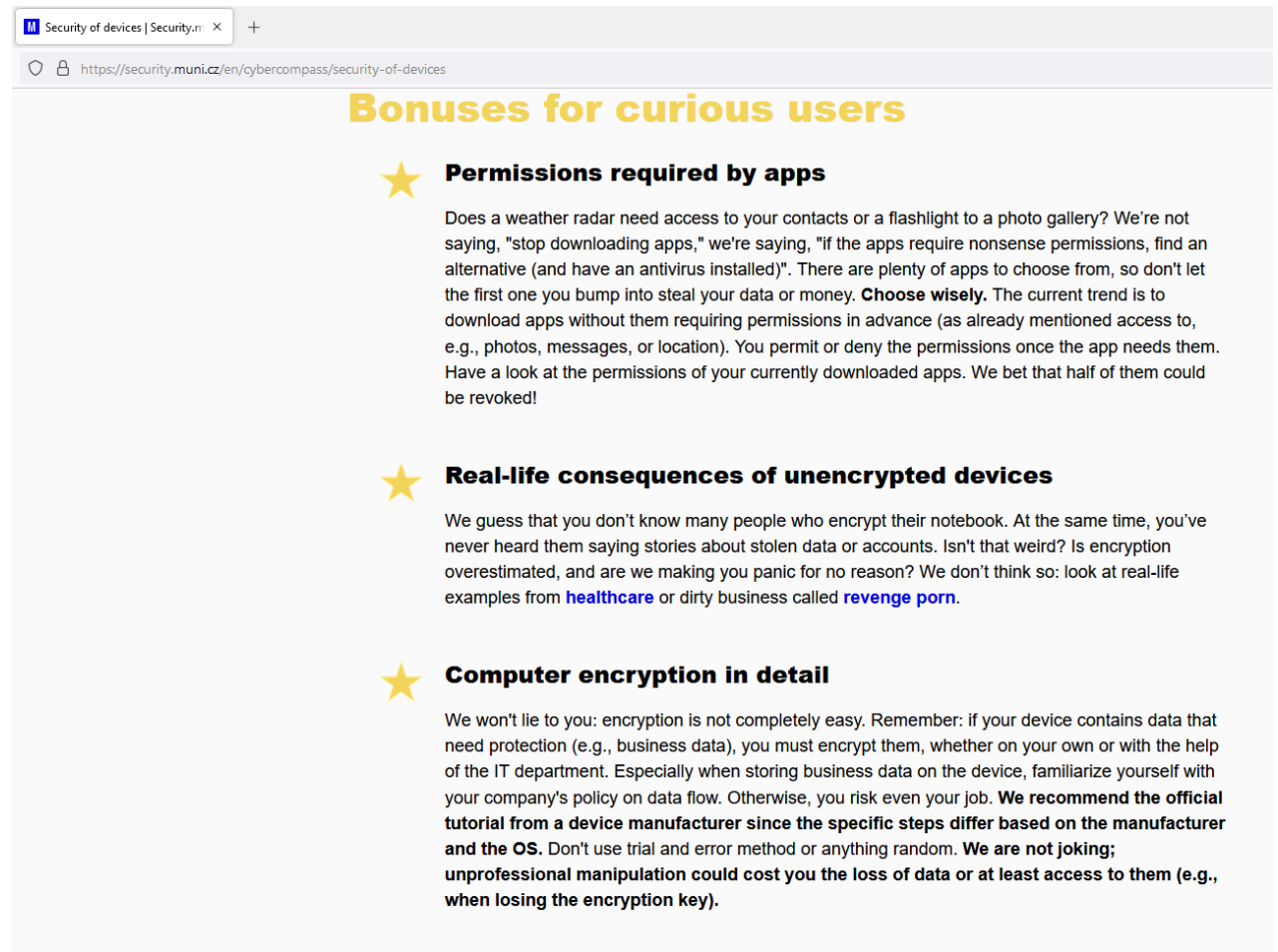
2 tutorials

An ounce of prevention is worth a pound of cure, right?

We all carry a smartphone, tablet, or laptop with us all the time. The risk of loss, theft, or another attack is therefore rising, and the consequences are usually fatal. Not to mention malicious code, which, of course, can attack your device wherever you are.

Lesson structure: Bonus Material

All lessons (except Incident reporting) contain bonus material at the end of the page.



Security of devices | Security.n x +
https://security.muni.cz/en/cybercompass/security-of-devices

Bonuses for curious users

- ★ **Permissions required by apps**

Does a weather radar need access to your contacts or a flashlight to a photo gallery? We're not saying, "stop downloading apps," we're saying, "if the apps require nonsense permissions, find an alternative (and have an antivirus installed)". There are plenty of apps to choose from, so don't let the first one you bump into steal your data or money. **Choose wisely.** The current trend is to download apps without them requiring permissions in advance (as already mentioned access to, e.g., photos, messages, or location). You permit or deny the permissions once the app needs them. Have a look at the permissions of your currently downloaded apps. We bet that half of them could be revoked!
- ★ **Real-life consequences of unencrypted devices**

We guess that you don't know many people who encrypt their notebook. At the same time, you've never heard them saying stories about stolen data or accounts. Isn't that weird? Is encryption overestimated, and are we making you panic for no reason? We don't think so: look at real-life examples from [healthcare](#) or dirty business called [revenge porn](#).
- ★ **Computer encryption in detail**

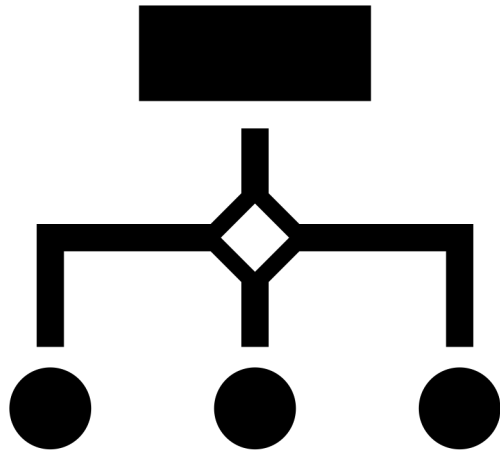
We won't lie to you: encryption is not completely easy. Remember: if your device contains data that need protection (e.g., business data), you must encrypt them, whether on your own or with the help of the IT department. Especially when storing business data on the device, familiarize yourself with your company's policy on data flow. Otherwise, you risk even your job. **We recommend the official tutorial from a device manufacturer since the specific steps differ based on the manufacturer and the OS.** Don't use trial and error method or anything random. **We are not joking; unprofessional manipulation could cost you the loss of data or at least access to them (e.g., when losing the encryption key).**



Cybercompass evaluation

We wanted to learn more about **students' attitudes** towards Cybercompass

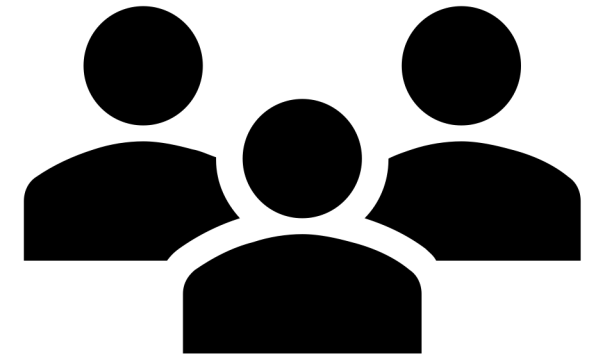
Evaluation procedure



- Mandatory **homework** of PV080 Information Security and Cryptography at Faculty of Informatics
- Asked students to **take the Cybercompass course** and answer a **questionnaire** after each lesson
- Students **received** 1.5% of total **points** of PV080 for taking the Cybercompass course and answering the related questionnaires
- Students could **opt-out** of their data being used for research purposes

Study participants

- **138 students** of PV080
- No opt-outs
- Data of 1–5 students per questionnaire excluded (did not answer reading check questions correctly)



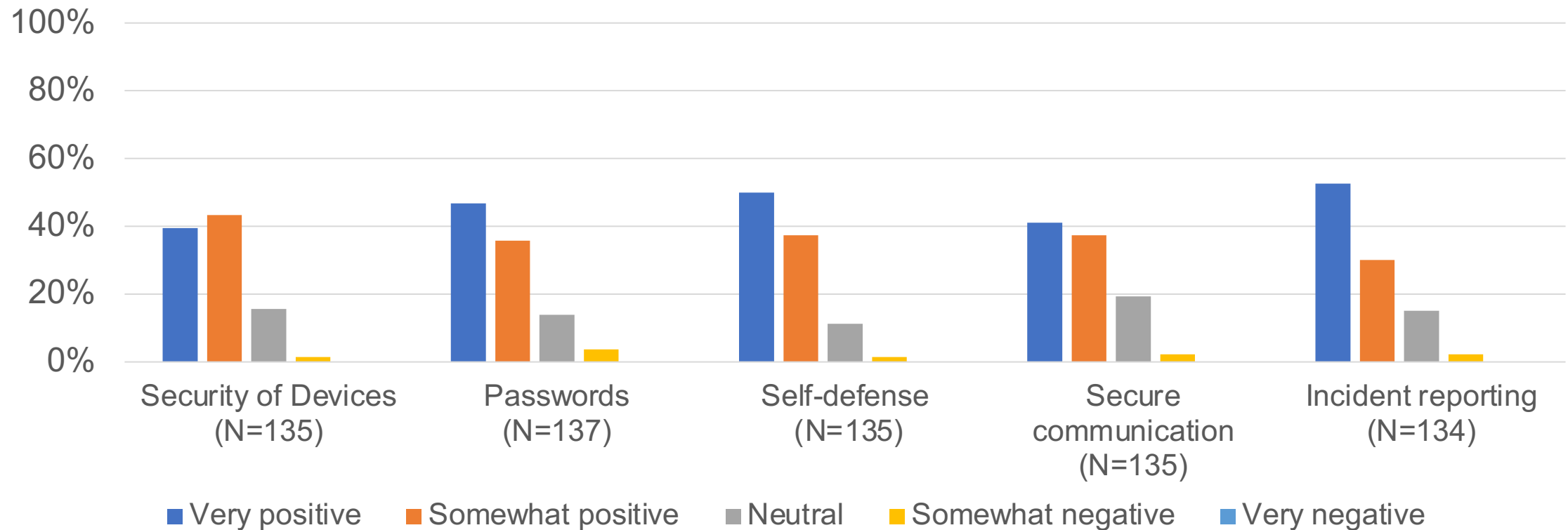
A vintage map with a grid of latitude and longitude lines is shown in the background. In the foreground, a brass compass rose is visible, featuring a central needle and four main directional points: North (N), East (E), South (S), and West (W). The compass face is marked with degrees from 0 to 360. The needle is pointing towards the North-Northwest direction. The overall scene is lit with warm, golden light, suggesting an old or historical setting.

Gained insights

Successes

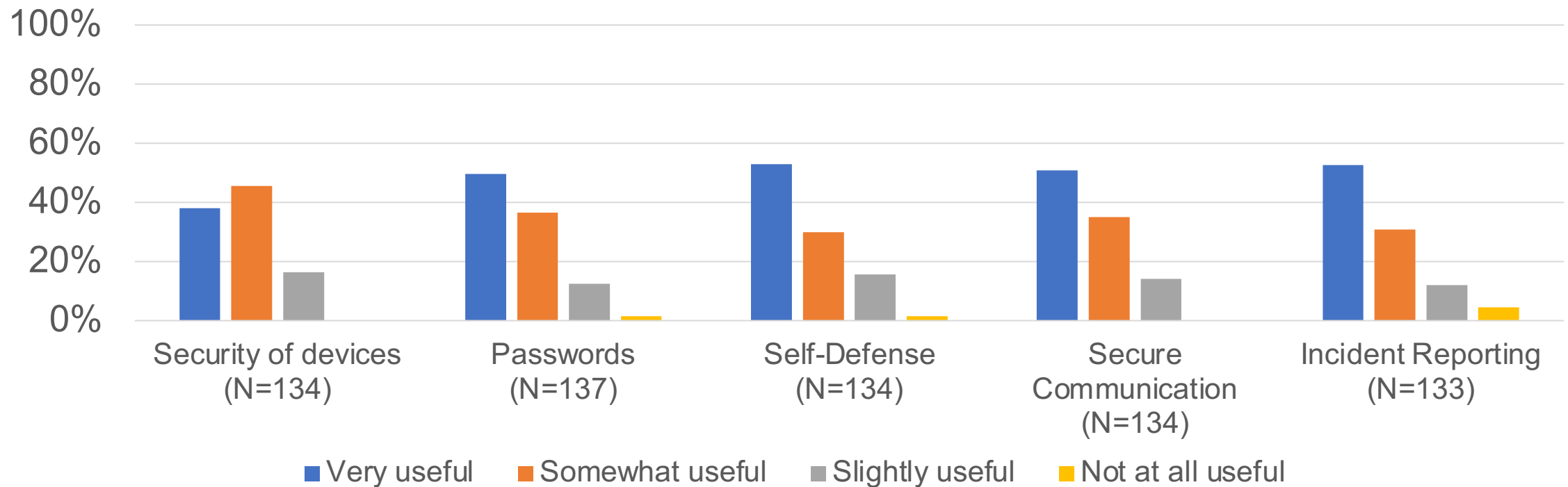
Lessons are perceived as positive

What is your overall impression of this lesson?



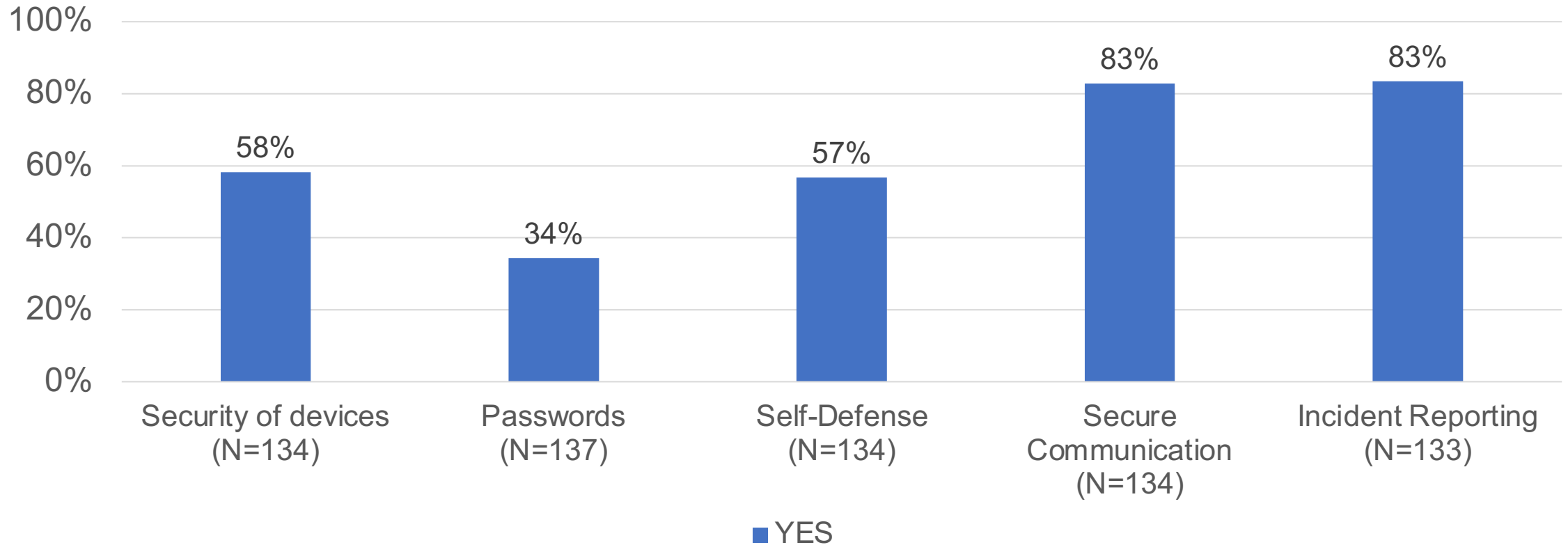
Lessons are perceived as useful

How useful did you find the information provided in this lesson?



Students learned new things in the course

Did you learn something new in this lesson?



Cybercompass lessons encourage action

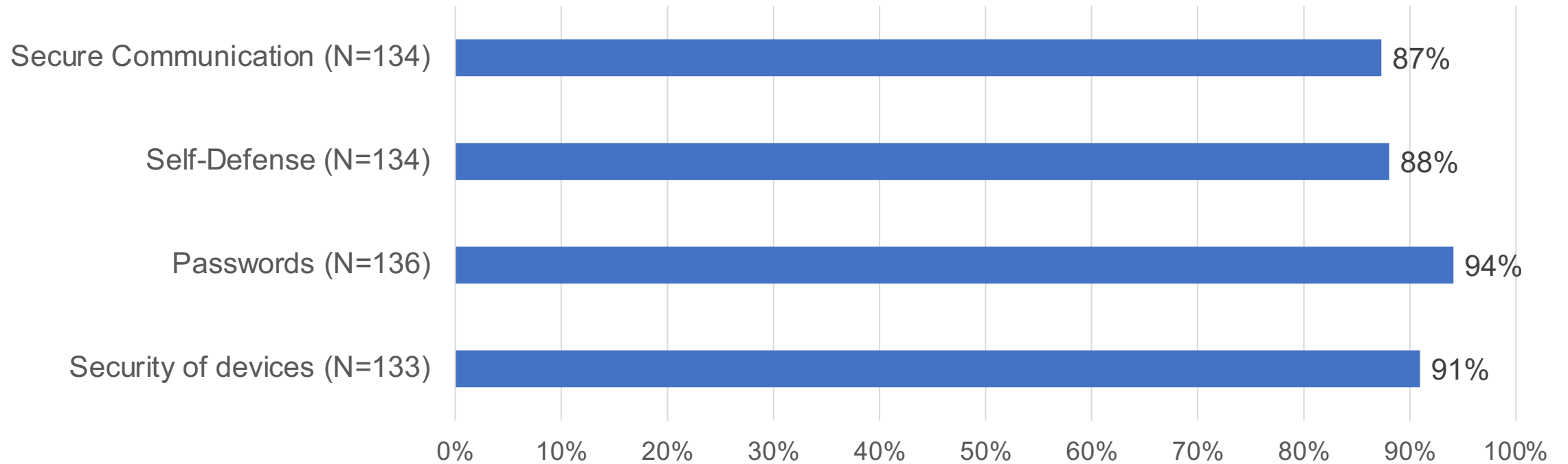
- “I changed my **notification preview** and as I am writing this **an encryption of my mobile** is running.” (Security of devices)
- “The lesson convinced me it is a good idea to **set up a password manager.**” (Passwords)
- “I liked especially the interactive part – **phishing quiz** which I will definitely remember for a long time.” (Self-defense)

Cybercompass lessons influence students' view on everyday cybersecurity

- **42%** said that Cybercompass **changed their view** on education and preparedness in terms of everyday cybersecurity
- Here's how:
 - "I gained an overall view on everyday security issues, and it made me **think more about security on a daily basis**"
 - "I will definitely **check the addresses of emails** more often"

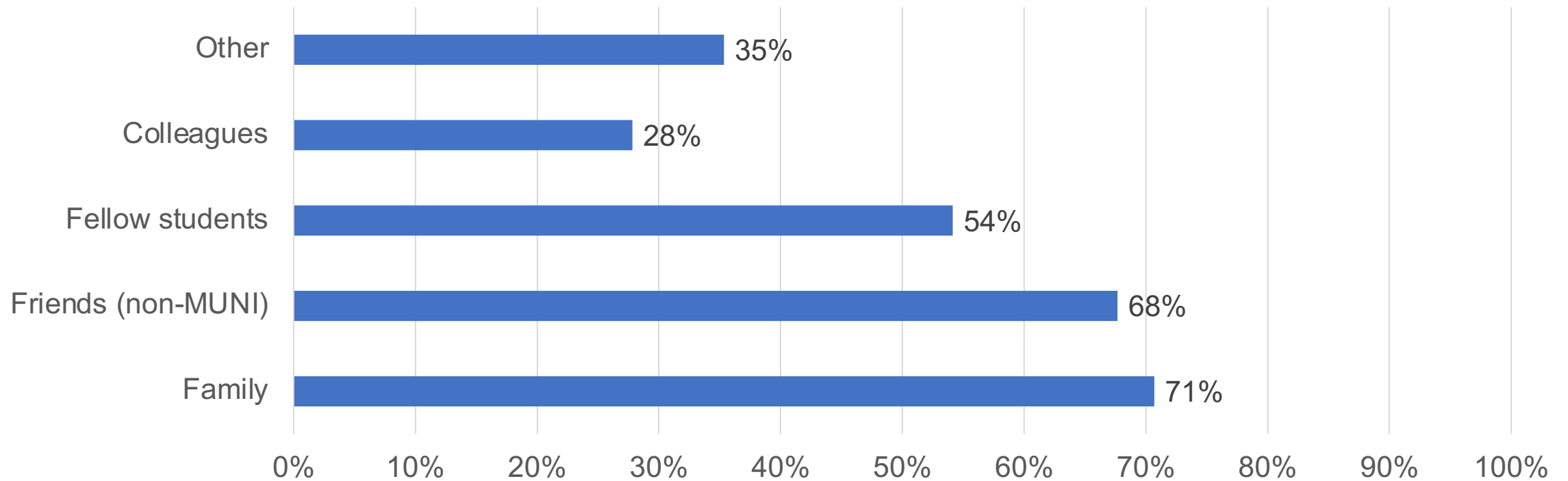
Bonus material is highly appreciated

Students who read the bonus material at least partially



Students are willing to recommend Cybercompass to others

Would you recommend the course to other people?



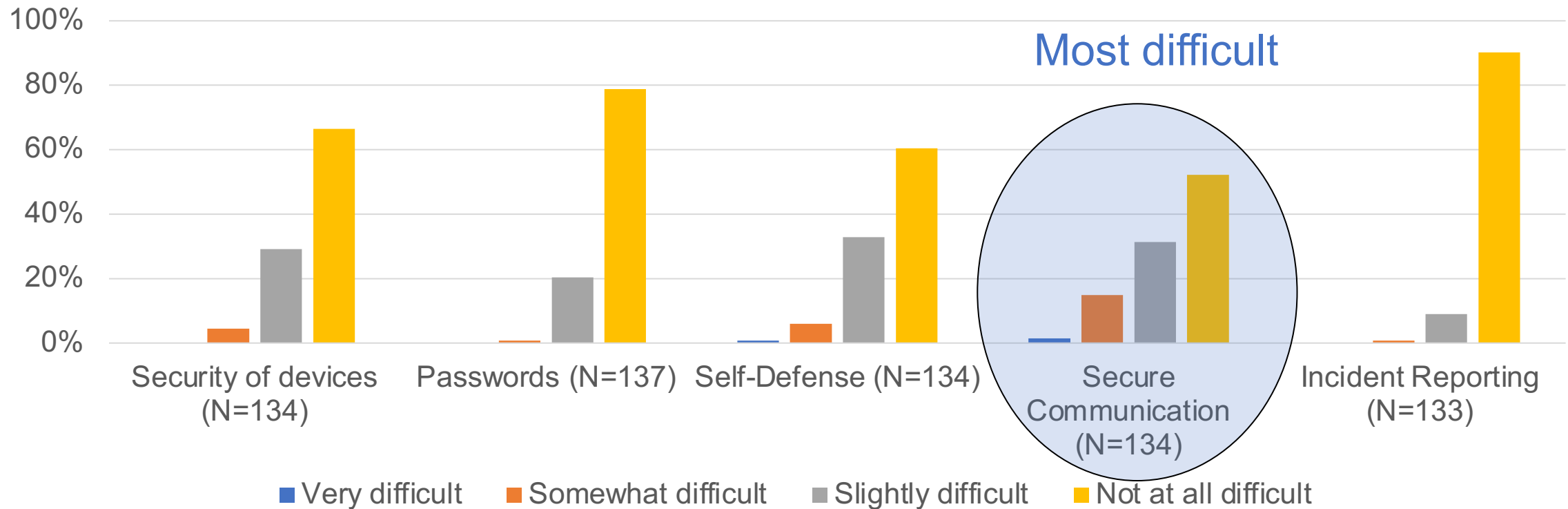
A vintage map with a grid of latitude and longitude lines is shown in the background. In the foreground, a brass compass rose is visible, featuring a central needle and a scale of degrees from 0 to 360. The compass rose is positioned over the map, and the needle points towards the top-left. The map shows various geographical features and text, including "St. Pierre", "St. Paul", and "St. Vincent".

Gained insights

Challenges

Lessons vary in difficulty I

How difficult did you find the information provided in this lesson?





Secure communication

Eduroam tutorial



Secure email @MUNI



Personal certificates



Email signing



Email encryption

MUNI services



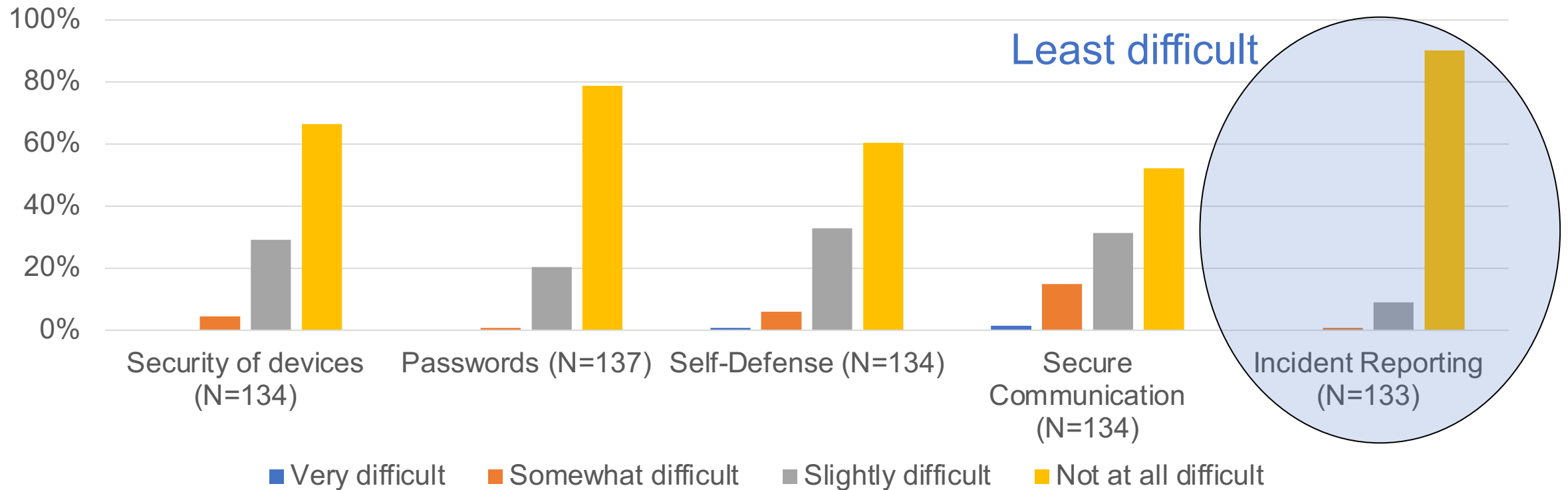
VPN



File sharing

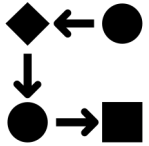
Lessons vary in difficulty II

How difficult did you find the information provided in this lesson?



Incident reporting

Incident reporting step-by-step



CSIRT-MU team

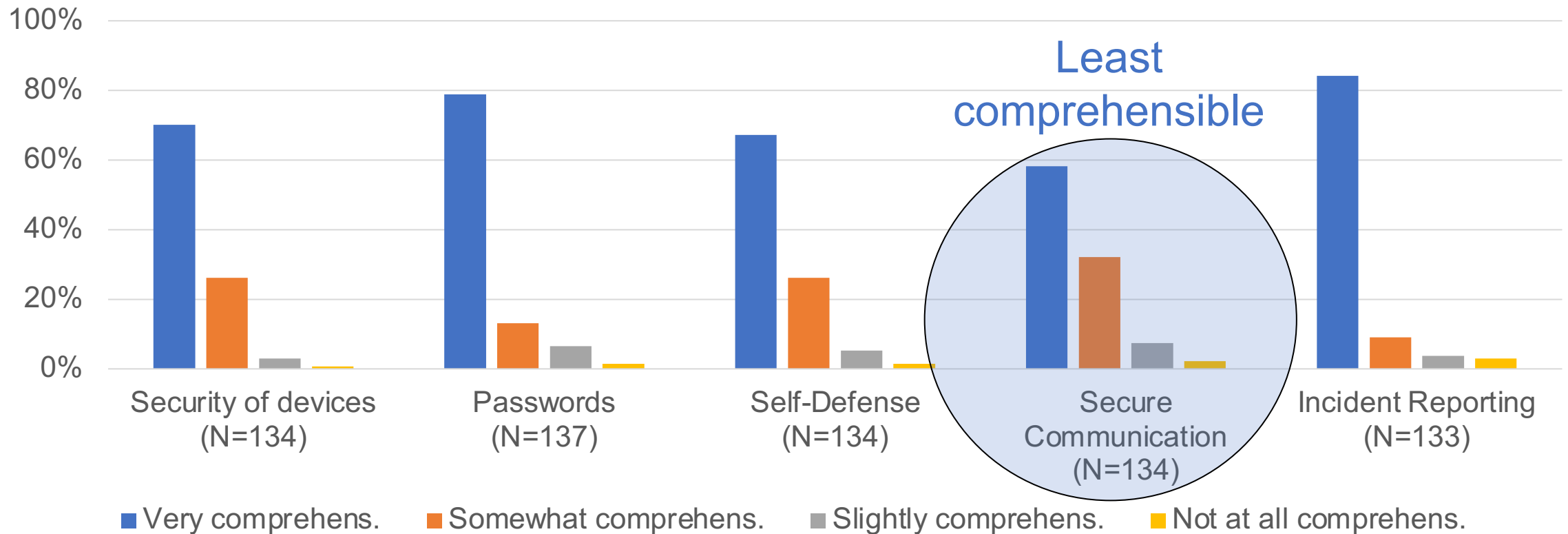


Contact information



Lessons vary in comprehensibility

How comprehensible did you find the information provided in this lesson?



Make all lessons accessible for the common user

- “This lesson is also well explained just like previous ones. However, I think it might be a little **bit difficult for ordinary user** to understand it.” (Secure communication)
- “I think this lesson can be for non IT person very difficult to understand because from my view it **includes too many technicalities**” (Secure communication)

Information on password managers and 2FA is insufficient

- “I’m not rating [the lesson] ‘very positive’ because I feel like **offline password managers should be mentioned**”
- “I’ve never used a password manager and what would really help me to convince me is **recommending a free (or very cheap) password manager, which wouldn’t be a hindrance, but an actual help**”
- “Maybe I would emphasize the use of the **two-factor authentication** more, I think it should be a standard these days, not something ‘more’.”

Most students have not heard about Cybercompass before

- **92%** of students had **not** heard of the course before
- The remaining 8% had heard of the course from:
 - Social media: LinkedIn and Facebook posts
 - News section of the internal study information system
 - (Physical) bulletins
 - A classmate
 - An external website



Takeaways

Recommendations for Course Designers and Security Educators



Recommendations for Course Designers

- Take MUNI's Cybercompass as an inspiration
- **Encourage action**
- **Include bonus material** for curious users
- **Evaluate** dissemination channels and **measure** reach

Recommendations for Security Educators

- Consider including topics of **everyday cybersecurity into your information security courses**
- Think of your **students as future cybersecurity advocates**
 - i. e. “individuals who encourage positive change by promoting and providing guidance on security best practices and technologies” (Haney & Lutters, 2017)

Summary

- Most students rated the individual lessons as **positive, useful, comprehensible and not difficult** at all!
- Even **IT students learned something new** in most lessons
- Students provided interesting **ideas** on how **to improve** the course
- Cybercompass is **freely available** at <https://security.muni.cz/en/cybercompass>
- [Full paper freely available](#)



More cybersecurity education research

Subscribe to our Twitter:  @cybersecmuni

Recent research papers:

- [Smart Environment for Adaptive Learning of Cybersecurity Skills](#) (IEEE TLT)
- [Capability Assessment Methodology and Comparative Analysis of Cybersecurity Training Platforms](#) (Computers&Security)

MUNI
C4E



EUROPEAN UNION
European Structural and Investment Funds
Operational Programme Research,
Development and Education



MINISTRY OF EDUCATION,
YOUTH AND SPORTS

C4E.CZ