CYBERSECURITY Awareness

Sharee English
Chief Security Officer

WECybr

Statistics

- The financial services industry contributed 62% of exposed data in 2019, though it accounted for only 6.5% of data breaches.

- In financial services, an average breach costs between $210 per record and $388 per record.

TOPICS

01

PERSONALLY IDENTIFIABLE INFORMATION (PII)

02

IDENTITY FRAUD/THEFT

03

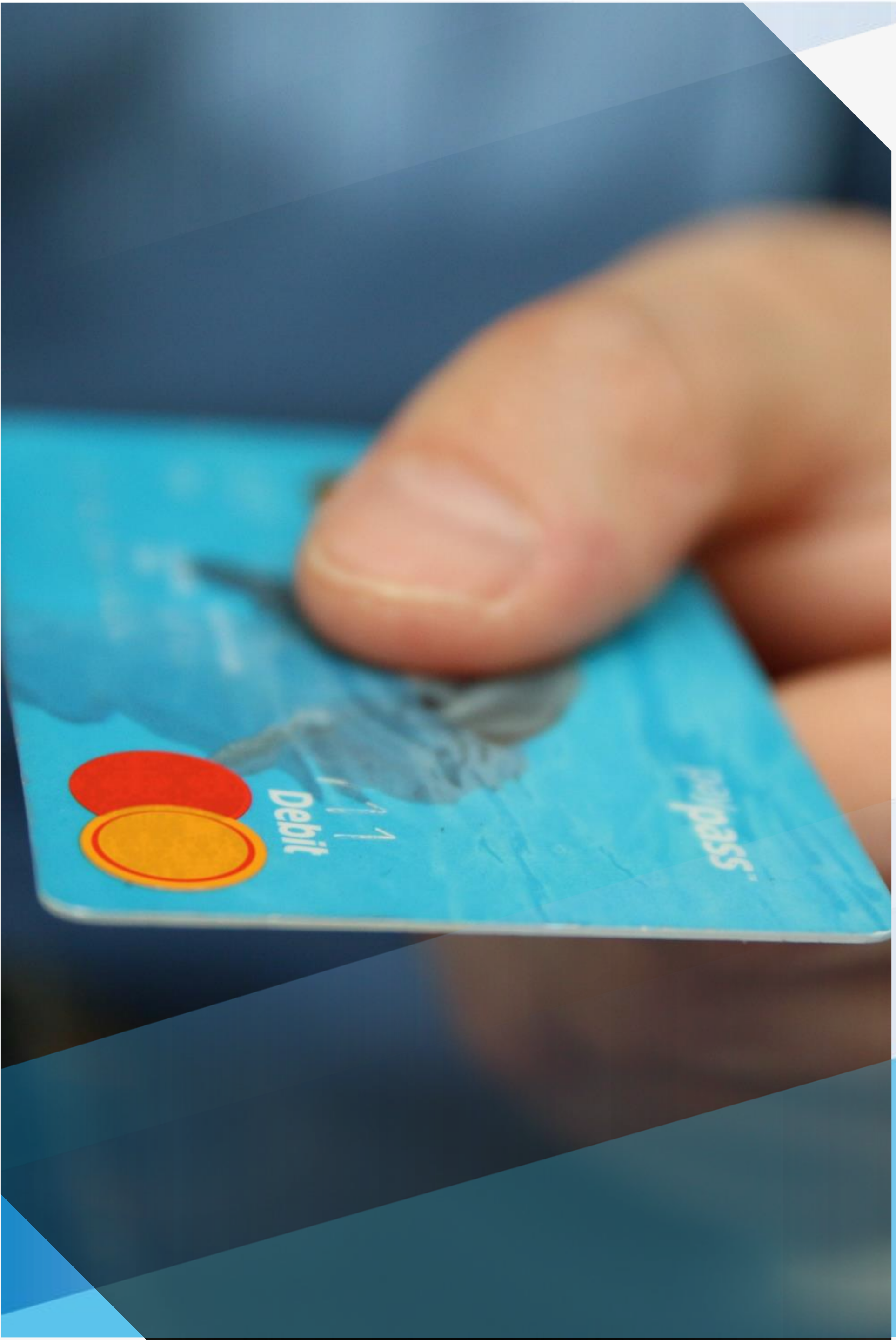
SOCIAL MEDIA

04

SOCIAL ENGINEERING

05

CYBERSECURITY WHILE TRAVELING



Personally Identifiable Information (PII)

Information in which you can identify an individual

- Name
- Address
- SSN
- Date of birth
- Place of birth
- Mother’s maiden name
- Biometric records
- Email address
- Passport number
- Driver’s license number
- Credit card numbers
- Telephone number
- Log-in details

Identity Crime Statistics

Every year in the U.S. over **19 million** people fall victim to identity crime

40% Age 20-29

18% Age 70+

Younger people reported losing money to fraud **more often** than older people

30%

Active social media users have a **30% higher risk** of becoming victims.

The average theft per victim is **$6,383.** The average **out of pocket expense** for the victim is **$422**

Identity Fraud Protection

- Use unique passwords
- Don’t overshare on social media
- Check your credit report regularly
- Monitor accounts often
- Secure your devices
- Have a plan in place in case of a breach

Digital Around the World in 2018

Important statistical indications for worldwide internet, social media, and mobile users.

TOTAL POPULATION	INTERNET USERS	ACTIVE SOCIAL MEDIA USERS	UNIQUE MOBILE USERS	ACTIVE MOBILE SOCIAL USERS
7.6 BILLION	4 BILLION	3.2 BILLION	5.1 BILLION	3 BILLION

Social Engineering

The use of deception to manipulate individuals into divulging **confidential or personal information** that may be used for fraudulent purposes (Wikipedia).

TOPICS

01 -ISHINGS

02 SHOULDER SURFING

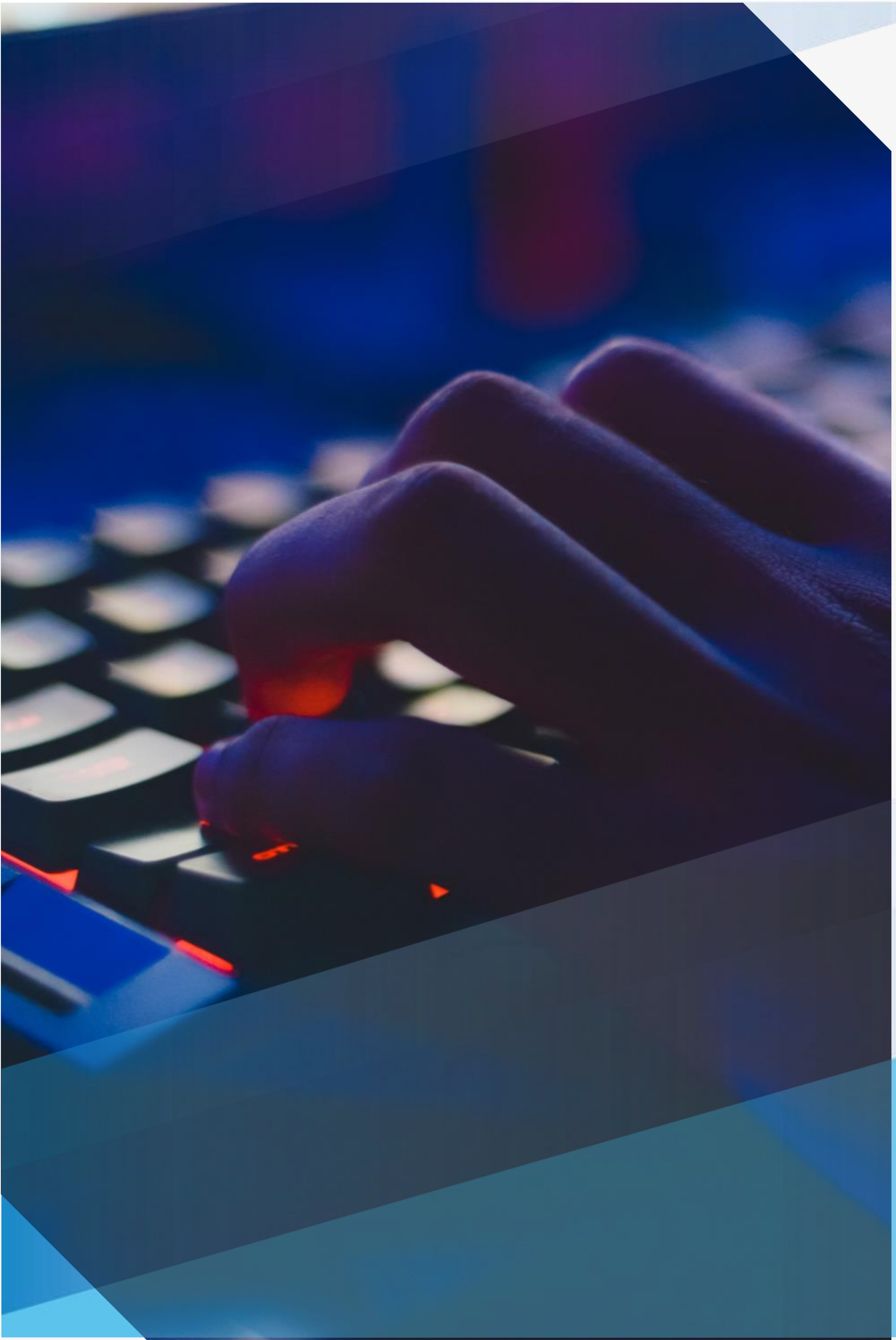
03 DUMPSTER DIVING

04 BAITING

05 TAILGAITING

06 WATER-HOLING

07 QUID PRO QUO



-Ishings

- Phishing
- Smishing
- Vishing

Phishing

- Convincing email
- Used to solicit information
- May install malware/virus

Phishing

Always verify information verbally

MITIGATION:

-Ishings

01

Employee training

02

Never call back on the number provided by the caller

03

Check mismatched URLs, grammatical errors and spelling mistakes

04

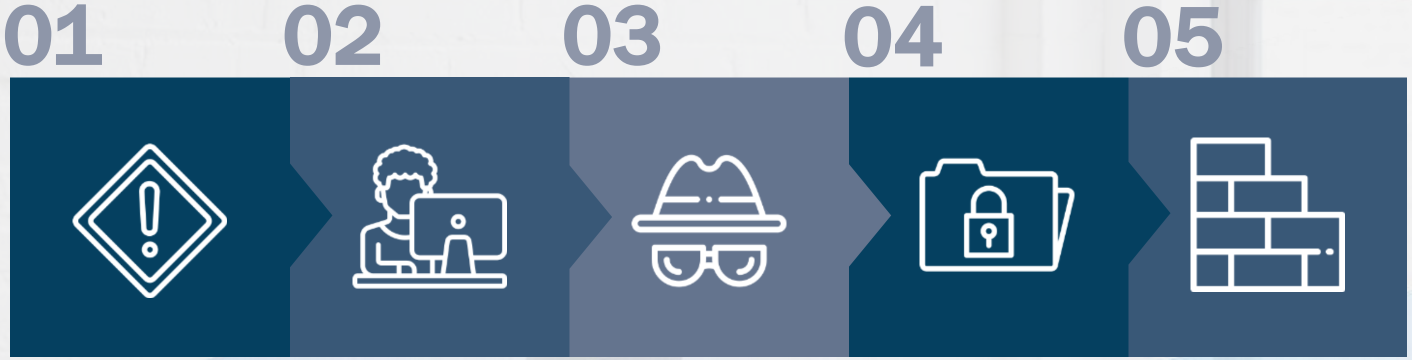
Notice alarmist tone intended to create fear

Shoulder Surfing

- **Key: Attacker has visibility to your screen and to your keyboard**
  - Criminal is positioned behind the victim
  - Attacker attempts to gather information as you type

MITIGATION:

Shoulder Surfing



01 Take precautions when entering information into devices

02 Angle computer screen or phone

03 Use privacy screens

04 Avoid opening sensitive files in public

05 Sit or stand with your back to a wall

Dumpster Diving

- **Using various methods to get information about a target victim.**
  - Going through the trash (actual garbage)
  - Recycle bin on your computer
  - Hard drive from thrown away computer
  - Discarded USB drives

MITIGATION:

Dumpster Diving

01

Use proper corporate approved method for discarding garbage

02

If garbage is left in office/cubicle be sure to lock

03

Wipe all devices clean prior to discarding

Baiting

- **Intentionally leaving malware-infected files/drives/devices**
  - Utilizes a person’s natural curiosity or lapse of judgement
  - Once device is inserted, it is set to autorun and starts infecting the computer or network

MITIGATION:

Baiting

01 Employee training

02 Use caution when new or foreign devices are introduced

03 Create a strong security culture

Tailgaiting

- **Also known as piggybacking**
- **A non-authorized user attempts to enter a secure area**
- Typical types of tailgaters
  - Disgruntled former employee
  - Thieves
  - Vandals
  - Mischief makers
- People with issues with an employee

MITIGATION:

Tailgaiting

01
02
03
04
05
06
07
08

01 Employee education

02 Photo ID required on entrance

03 Use of smart cards

04 Multi-factor authentication

05 Security guards

06 Biometrics

07 Turnstiles or other mechanism to limit entrance to a single person at a time

08 Ensuring doors close behind each individual

Cybersecurity while traveling

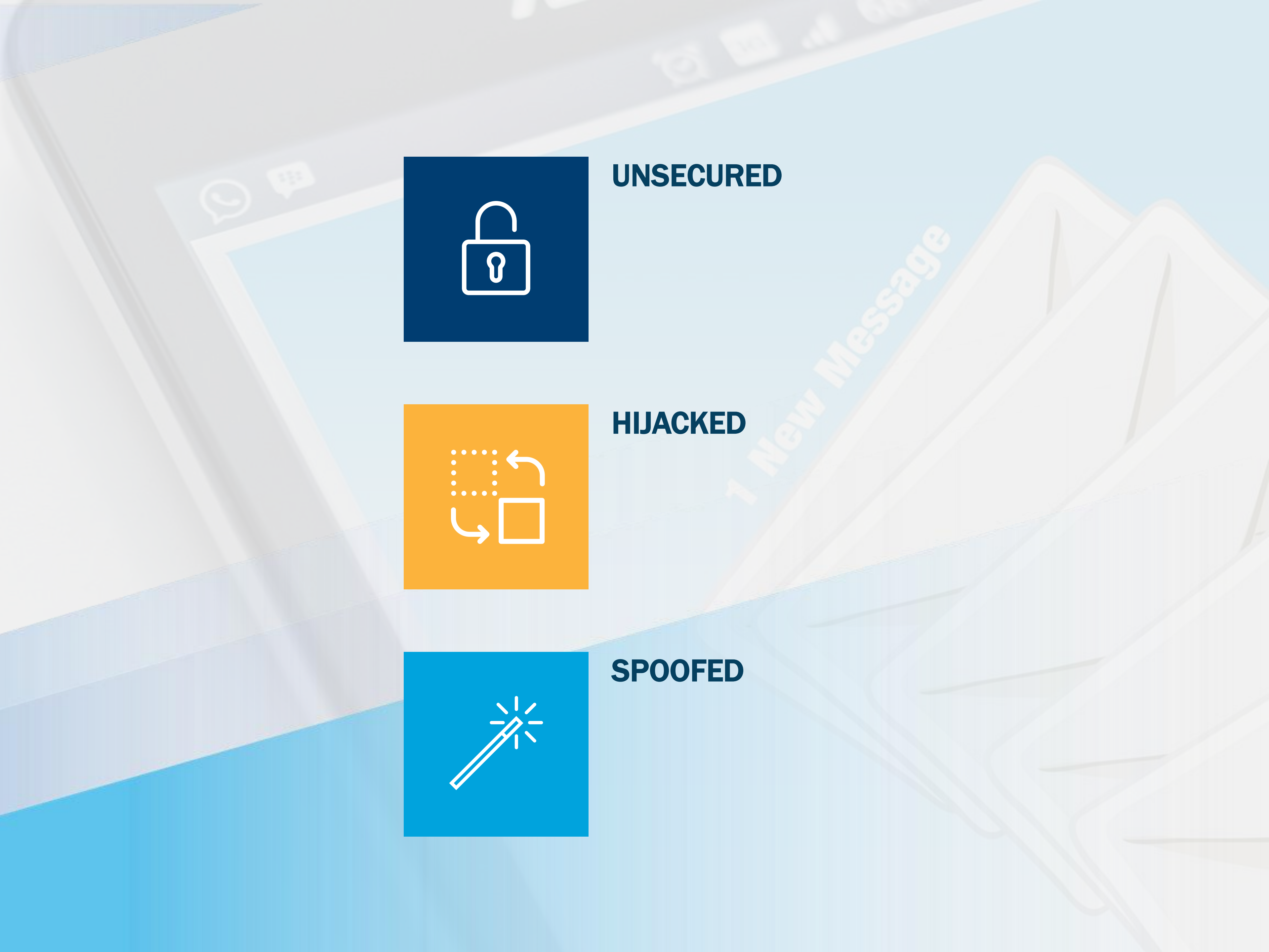
THREATS

- Wireless Networks
- Juice Jacking
- Theft

PREVENTATIVE MEASURES

- Passwords and Passcodes
- Disable Auto-connect
- Disable Bluetooth
- Utilize Encryption
  - Disk Encryption
  - Website Encryption
  - VPN
- Perform Updates

Wireless Networks



UNSECURED

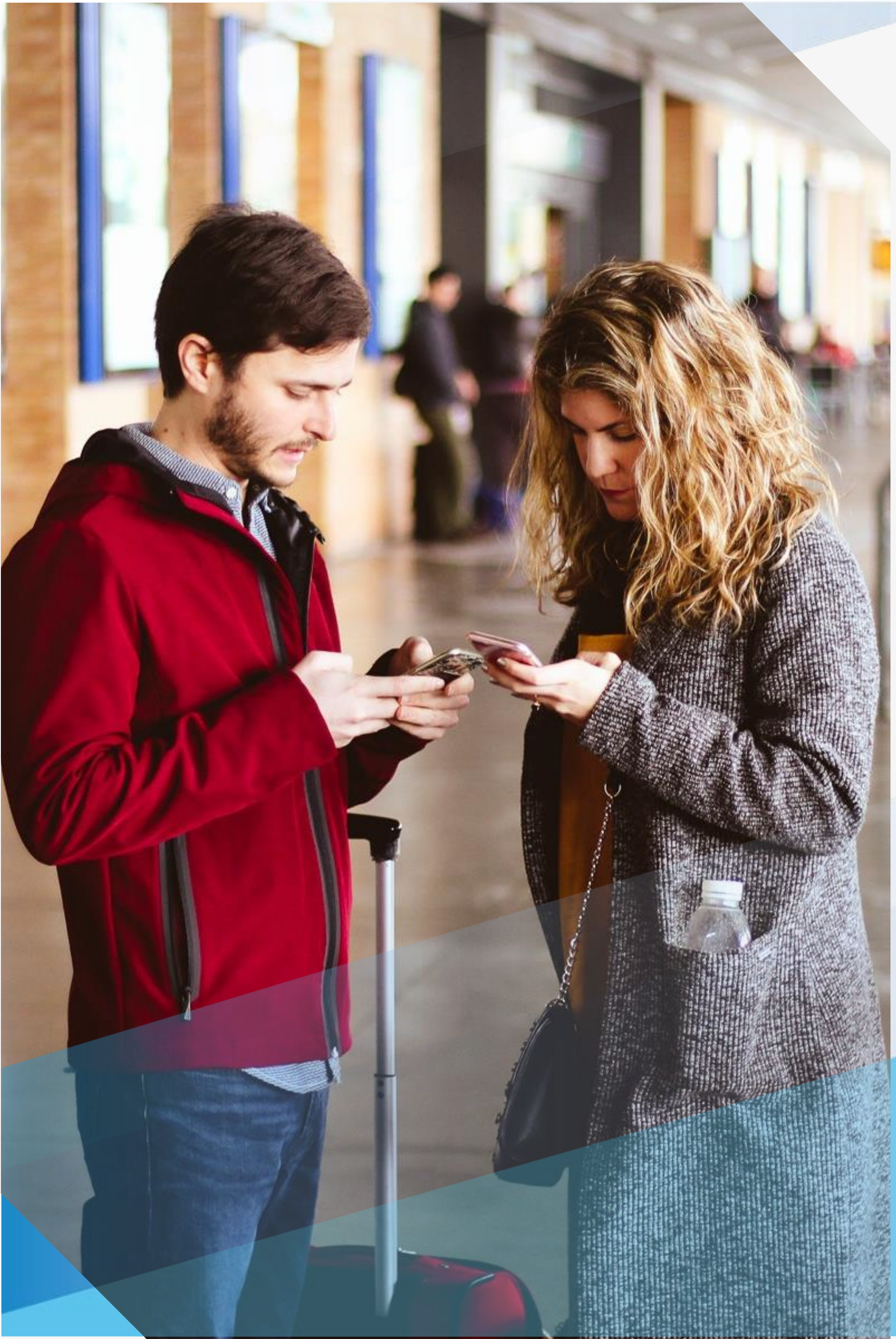
HIJACKED

SPOOFED

Juice Jacking

FREE CHARGING STATIONS

STEAL SENSITIVE INFORMATION



Prevention

- Use Passwords/Passcodes
- Disable Auto-connect
- Disable Bluetooth
- Use Encryption
- Perform Updates
- Be Aware of your Surroundings

THANK YOU!

Sharee English

WECybr