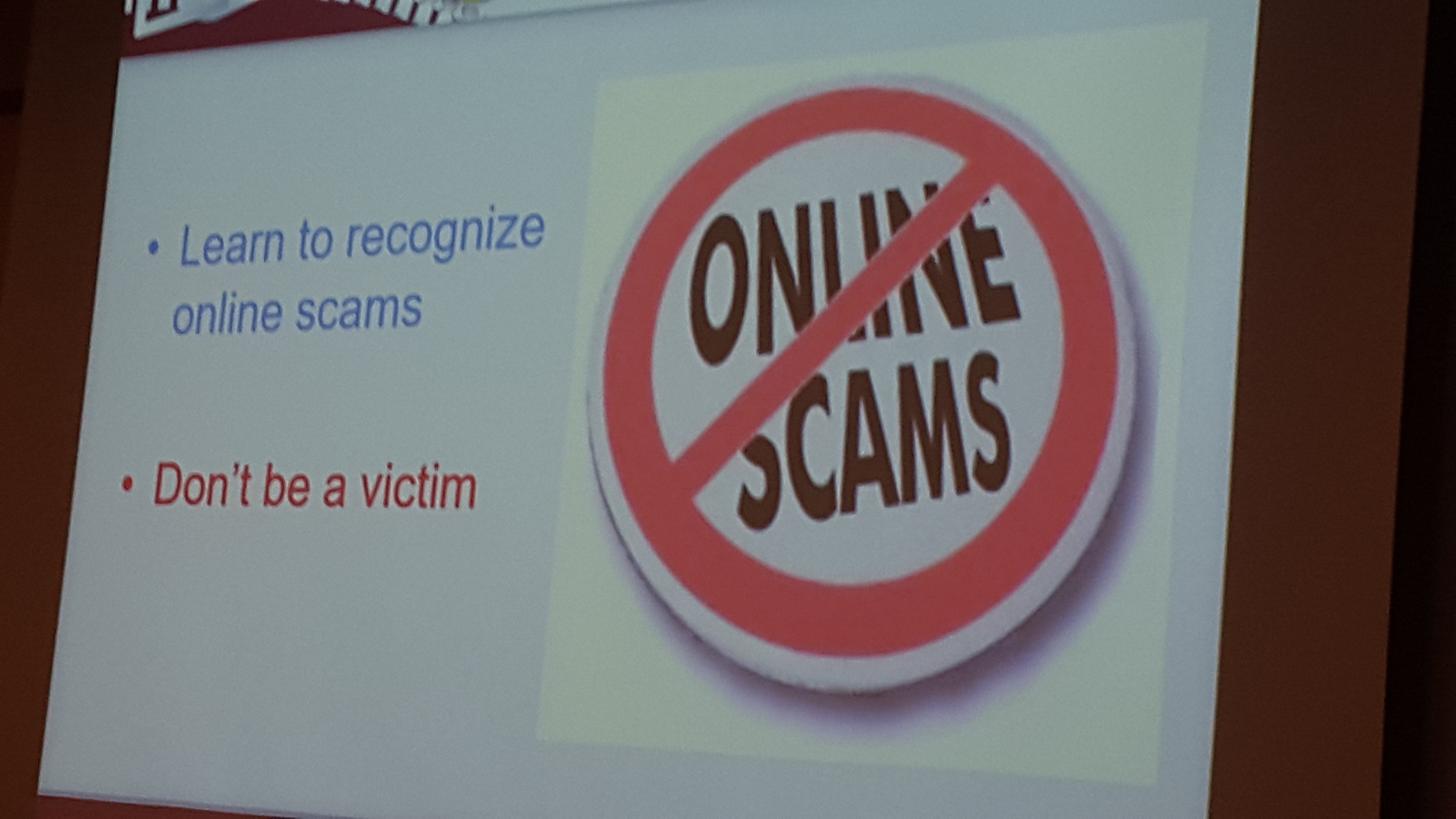
|  |
| --- |
| **Malmö International Rotary Club 2390 *2020 Febr 24*** |

**Subject: Fraud >--< Internet**



**Speaker: Liban Abanur, born 1980 in Somalia, MIRC member**

**Liban A. works with multinational organizations and companies, with managing, guiding and project development. His background is within the fields of leadership, integration, diversity, managing, project development, Network Security, Management and troubleshooting of core data-center devices such as Routers, Switches and IT infrastructure. He holds AP diploma of Network Engineering and a Bachelor of Product development and integration technology from the Copenhagen School of Design and Technology and is a Candidate of second master’s Program in Information Security System at Linnaeus University.   
He began his career working for the Spanish Administration in Saudi Arabia. During his almost seven years’ tenure as administrator, he covered five markets: Bahrain, Kuwait, Oman, Saudi Arabia and Yemen, and managed hundreds of successful commercial trade missions on behalf of bilateral commercial in both directions.**

**---------------------------------------------------------------**

In computer [software](https://en.wikipedia.org/wiki/Software), business logic or domain logic is the part of the program that encodes the real-world [business rules](https://en.wikipedia.org/wiki/Business_rule) that determine how data can be [created, stored, and changed](https://en.wikipedia.org/wiki/Create,_read,_update_and_delete). It is contrasted with the remainder of the software that might be concerned with lower-level details of managing a [database](https://en.wikipedia.org/wiki/Database) or displaying the [user interface](https://en.wikipedia.org/wiki/User_interface), system infrastructure, or generally connecting various parts of the program.

Business logic should be distinguished from business rules. The scammer will typically attempt to get the victim to allow remote access to his or her computer. After remote access is gained, the scammer relies on [confidence tricks](https://en.wikipedia.org/wiki/Confidence_trick), typically involving utilities builtinto Windows and other software, in order to gain the victim's trust to pay for the supposed "support" services. The scammer will often then steal the victim's [credit card](https://en.wikipedia.org/wiki/Credit_card) account information or persuade the victim to log into his or her online banking account to receive a promised refund, only to steal more money, claiming that a secure server is connected and that the scammer cannot see the details. Many schemes involve convincing the victim to purchase expensive [gift cards](https://en.wikipedia.org/wiki/Gift_card) and then to divulge the card information to the scammer. Telemarketing fraud is [fraudulent](https://en.wikipedia.org/wiki/Phone_fraud) [selling conducted over the telephone](https://en.wikipedia.org/wiki/Telemarketing). The term is also used for telephone fraud *not* involving selling.

Telemarketing fraud is one of the most persuasive deceptions identified by the [Federal Trade Commission](https://en.wikipedia.org/wiki/Federal_Trade_Commission) (FTC). Telemarketing fraud often involves some sort of victim compliance whether it involves the victim initiating contact with the perpetrator or voluntarily providing their private information to the offender; thus, fraud victims may experience feelings of shame and embarrassment that may prevent them from reporting their victimization.

**Older people are disproportionately targeted by fraudulent telemarketers and make up 80% of victims affected by telemarketing scams alone. Older people may be targeted more because the scammer assumes they may be more trusting, too polite to hang up, or have a nest egg.**

**Service above self 😊 INGVAR**