Can we say the most common way to authenticate is secure nowadays ?

Today, the most common way to authenticate is the use of logins and passwords. But, there are lots of hacker attacks every single day. It results lots of companies lost theirs databases which hold personal informations of clients (like passwords for example). We can use the example of Yahoo which has the informations of 3 billions of clients are published on Internet.
The most common way to authenticate is secure nowadays?
We will understand why our actual mean of authentication can show issues. Then, we will explain others ways which could be used more frequently. **(1min30)**

Let me introduce our subject with few reminders. With all dangers on Internet, the IT Security has 3 goals :

- the confidentiality : this aspect means only the sender and the receiver of the message must understand the content of this message.
- the integrity : the integrity implies noone modified the message sent to the receiver
- the authenticity : this aspect means the identity of the sender is verified before the recipient read the message

So, on a website for example, the authentication uses the authenticity because we need to prevent anyone from connecting on any user account. And, the website must use verify the secure authentication. But how ? **(1min30)**

Firstly, a web service can not store plaintext passwords and uses hash functions. These hash functions allows to transform a message M into an other message H. Fortunalety, we can not transform the message H into the message M.
So, web service must use this method to store and verifiy his passwords. When a user wants to connect to the service, he writes his password. Then, on the client side, the hash of the password is calculate. Finally, the web service verifies the hash of the client with the content of his database.
If this technique is not used by the web service, the authentication could be prejudiced. In fact, if the database is attacked then the hacker will have the plaintext passwords of clients. An other technique (with less resources), it is seeing the password of the victim with a look over his shoulder **(2min)**

Moreover, the nature of the password chosen by the user can be problematic. In fact, hackers have a list of passwords used a lot. So, when they make an attack, hackers used this list to find the proper password : it is the dictionary attack.
For instance, this screen shows WPA-2 attack which consists to find the Wifi Password. The attack consists of sniffing packets sent in the network. Then, with the authentication of the device, we can calculate the password with the challenge-response sent. Here, the password was too easy to find out.
Unfortunately, even if your password for an application is complex, if you use the same for few services, it is a risk for your authentication. In fact, if a web service is attacked, the hackers will add the found passwords in their dictionnary for others applications. **(2min)**

We can say the authentication is strong when there are 2 different types of authentication :

- what I know : it is the use of a password in the most of the cases
- what I have : it is an object like a key, a card or a cellphone for example
- what I am : it is the use of your fingerprints, voiceprints or retinal scans

Nowadays, the bigger websites of social networks (like Facebook for example) use the two-factor authentication with the password and the sending of an SMS message.
So, the use of this technique allows to improve the security of the authentication. **(1min30)**

In conclusion, we can say the most common way to authenticate is secure nowadays. In fact, the only use of passwords for web services especially makes the authentication not secure. Because, most people use the same weak password. So, we have to ask ourselves what laws voting to improve the security on Internet. **(1min 30)**