DigiSkiPasS – Digital Skills Passport for Senior

2023-1-BE01-KA210-ADU-000153530

www.digiskipass.com

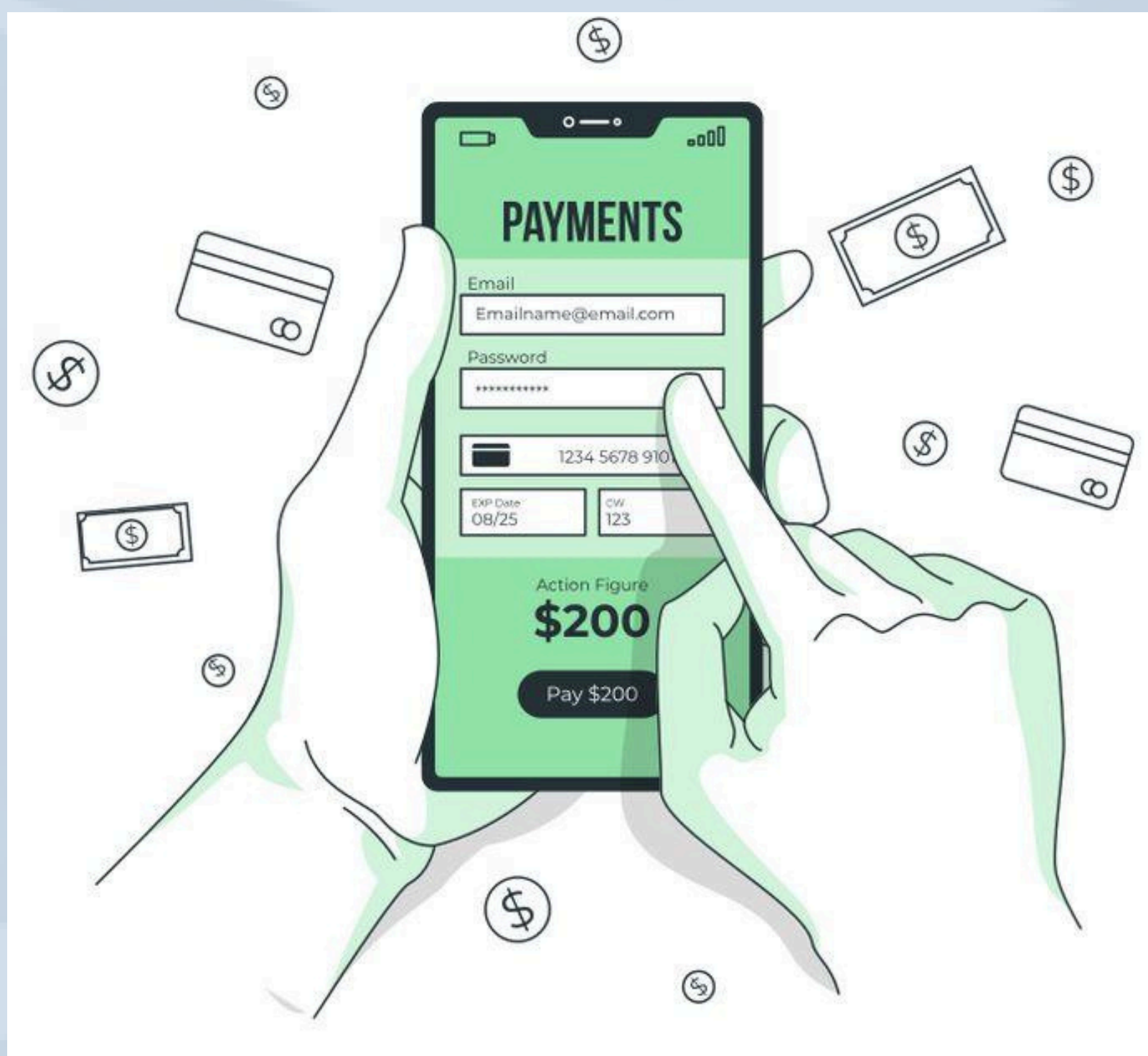# INTERNET BANKING

INTRODUCTION TO INTERNET BANKING

Internet banking, also known as online banking, is a convenient way to manage your finances through a computer. It allows you to perform various banking operations such as checking account balances, making payments and transfers, managing credit and debit cards, and more.

If you're interested in using online banking, you may want to explore what your local bank has to offer. They provide secure access to your account and a range of features to help you manage your money efficiently. Remember to keep your banking details safe at all times and watch out for phishing attempts.

SETTING UP ONLINE BANKING

Setting up online banking usually involves a few key steps:

1. **Sign up online:** Visit your bank's website and look for the option to sign up or sign up for internet banking.
2. **Identity verification:** Provide the necessary identifying details, which may include your social security number, account number, or other personal information.
3. **Create credentials:** Choose a secure username and password according to the bank's guidelines.
4. **Security verification:** Complete any additional security checks required by the bank, which may involve answering security questions or confirming a code sent to your phone or email.
5. **Confirm:** Once you have completed these steps, you will receive confirmation that your internet banking setup is complete.

For step-by-step instructions, it's best to follow the specific instructions provided by your bank, as each institution's process may differ slightly. If you need help, most banks offer customer support through their website or helpline. Remember to keep your login details private and secure.
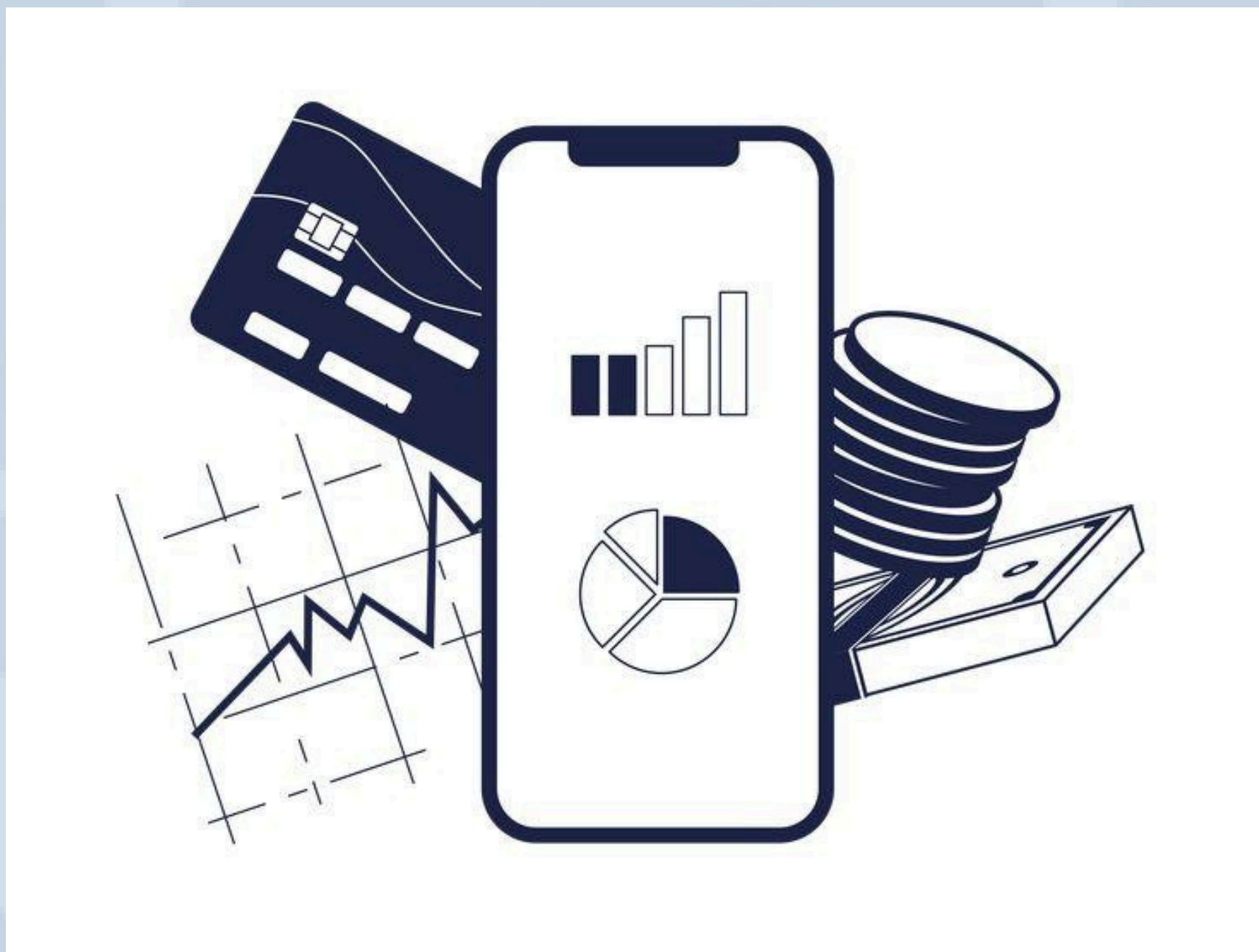
DIFFERENCES BETWEEN INTERNET AND MOBILE BANKING.

Yes, mobile banking and internet banking are different, although they are related concepts. Here's a quick comparison:

Smartphone banking:

- Performed using a mobile telecommunications device (such as a smartphone or tablet).
- Accessible via mobile app or SMS.
- Designed for mobile banking such as checking balances, transferring funds, or paying invoices or bills.
- It may have restrictions on transactions or provide more limited services than online banking.

Online banking:

- Via the Internet using a personal computer, but can also be accessed via mobile browsers.
- They often provide more comprehensive banking services.
- Suitable for more complex banking tasks, such as applying for a loan or managing investments.
- Higher transaction limits are usually allowed.

Both forms of banking offer convenience and flexibility, allowing you to manage your finances remotely. However, the choice between them may depend on your specific needs and the type of trades you intend to make.

Mobile banking incorporates various security measures to protect users' financial information and transactions.

Here are some of the main commonly used security features:

- **Encryption:** The data transmitted between your mobile device and the bank's servers is encrypted, making it difficult for unauthorized parties to intercept and read your information.
- **Two-factor authentication (2FA):** Adds an extra layer of security by requiring two forms of authentication before access is granted, typically by combining information you know (such as a password) with information sent to you (such as a timecode sent to your phone).
- **Biometric verification:** Many mobile banking apps now use fingerprint scanning, facial recognition, or voice recognition to verify your identity.
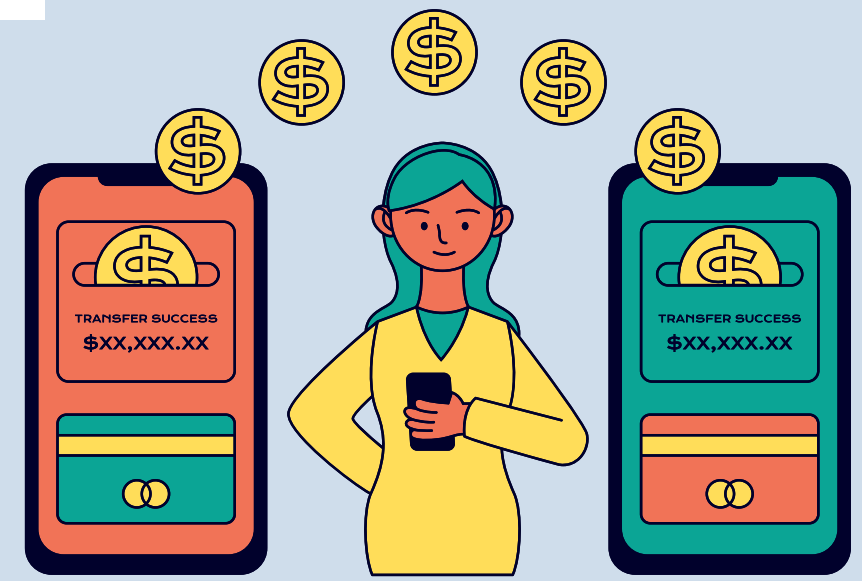
- **Automatic logout:** To prevent unauthorized access, mobile banking apps often automatically log you out after a period of inactivity.

- **Fraud detection systems:** Banks use sophisticated systems to monitor for unusual activity that could indicate fraud.
- **Security alerts:** You can receive alerts for transactions, login attempts, and other significant account activity.
- **Regular software updates:** Keeping the banking app up-to-date ensures that you have the latest security features and fixes.

It's also important for users to follow best practices: for example, use strong passwords, avoid using public Wi-Fi for banking, and keep your mobile device's software up to date. Always download banking apps from official app stores and be wary of phishing attempts and suspicious links. Remember, keeping your mobile banking experience secure is a shared responsibility between you and your bank.