FRAUD PREVENTION

How to keep your information secure

CYBER FRAUD IS ON THE RISE...

Did you know:

47% of American adults have had their personal information exposed by cyber criminals.

1 in 3 homes with computers are infected with malicious software.

65% of Americans who go online have received at least one online scam offer.

WHAT IS PII?

PII, otherwise known as personally identifiable information, is data that may be used to identify a certain individual. Examples of this information are...

- Full name
- Social Security Number
- Driver's license number
- Bank account number
- Passport number
- Email address

PII is what cyber criminals use to commit identity theft. You should take precautionary steps to safeguard this information.

Source: LifeLock by Norton | www.lifelock.com/learn/identity-theft-resources/what-is-personally-identifiable-information

HOW CAN I KEEP MY PII SAFE?

Criminal access to your PII is what makes identity theft and fraud possible. Therefore, you should take steps to safeguard this information.

PHYSICAL DOCUMENT SECURITY

Physical documents that include your PII should be handled with care. Be sure to shred documents with identifying information on them before discarding. Government documents containing your PII (ex. Driver's licenses, birth certificates, Social Security cards, etc.) should be stored in a secure location that you do not disclose with others.

Source: LifeLock by Norton | www.lifelock.com/learn/identity-theft-resources/what-is-personally-identifiable-information

ONLINE BANKING SECURITY

Monitor your financial accounts and transactions regularly. If you notice activity that seems suspicious, notify your financial institution immediately.

Source: Cybersecurity & Infrastructure Security Agency | www.cisa.gov/be-cyber-smart/your-personal-information-protecting-it-exploitation

PASSWORD SECURITY

It is almost guaranteed that at least one of your passwords, past or present, has been exposed by a data breach. Follow these tips to create stronger passwords that are more resistant to data breaches:

- Don't reuse passwords
- Make passwords at least twelve characters in length, including a combination of upper- and lower-case letters, numbers, and symbols.
- Consider using a trustworthy password manager such as Lastpass, 1Password, or Keeper. A password manager is a program that stores and encrypts your passwords, making them less susceptible to data breaches. They can also generate random passwords that are difficult to guess or hack.

Source: KnowBe4

united bay community credit union

RESOURCES

REPORT FRAUD - ReportFraud.ftc.gov.
EXPLORE DATA - ftc.gov/exploredata.
REPORT IDENTITY THEFT - IdentityTheft.gov
COMMON SCAMS - usa.gov/common-scams-frauds