Country Club Bank Member FDIC
epcor Electronic Payments Core of Knowledge
PAYMENTS INSIDER
The inside scoop on payments for businesses of all sizes

Protecting Your Identity: A Crucial Guide to Safeguarding Your Personal Information

In today's digital age, where technology permeates nearly every aspect of our lives, the threat of identity theft looms larger than ever before. Did you know that more than 40 million U.S. consumers fell victim to some form of identity theft in 2021 alone?

Shockingly, according to Javelin's research, traditional identity fraud losses surged to a staggering $24 billion in 2021, marking a disturbing 79% increase over the previous year. When combined with losses from scams where individuals unwittingly provide personal information, the total losses soared to a staggering $52 billion.

Identity theft occurs when someone unlawfully uses your personally identifiable information (PII) for their own gain. This includes sensitive data such as social security numbers, credit card details and dates of birth. With our lives increasingly intertwined with the digital realm, protecting this information has never been more critical. Whether it's healthcare data, financial details or even the identities of our children; no one is immune to the risks posed by malicious actors lurking in the virtual shadows.

Understanding the various forms of identity theft is the first step towards safeguarding yourself and your loved ones. From medical and financial identity theft to the alarming rise of synthetic identity theft, where fraudsters create fictitious identities using fragments of real information, the threats are multifaceted and ever-evolving.

So, what can you do to minimize the risk of falling victim to these insidious crimes? Here are ten proactive measures you can take to fortify your defenses against identity theft:

1. **Utilize Strong Passwords:** Embrace the mantra of unique, complex passwords for each online account, and consider employing a password manager for added security.
2. **Exercise Caution with Public Wi-Fi:** Avoid accessing sensitive accounts over public networks, as they are prime hunting grounds for cybercriminals.
3. **Manage Bluetooth Usage:** Disable Bluetooth when not in use to prevent unauthorized access to your devices.
4. **Secure Your Mobile Devices:** Protect your smartphones with passwords or biometric authentication, and be mindful of the apps you install.
5. **Keep Software Updated:** Regularly update your devices' software and firmware to patch vulnerabilities exploited by cybercriminals.
6. **Monitor Financial Accounts:** Stay vigilant by reviewing your account statements regularly and setting up alerts for suspicious activity.
7. **Guard Your Mailbox:** Be mindful of the sensitive information that arrives in your physical mailbox and take steps to secure it, especially when traveling.
8. **Consider Freezing Your Credit:** Temporarily freeze your credit to prevent unauthorized access and regularly review your credit reports for any irregularities.
9. **Protect Your Social Security Number:** Safeguard this vital piece of information by limiting its exposure and verifying the legitimacy of requests for it.
10. **Safeguard Your Children's Information:** Shield your children from identity theft by securing their social security numbers and educating them about online safety.

While we cannot completely eradicate the threat of identity theft, staying informed and proactive can significantly reduce the risk. By implementing these measures and remaining vigilant, you can fortify your defenses against cyber threats and mitigate potential losses.

Stay safe, stay informed, and together, we can combat the scourge of identity theft in our increasingly interconnected world.

Did you spot the scams? If so, you're a total fraudbuster!

Test your knowledge by identifying if the following scenarios are fraud or legitimate.

Question 1: You receive an email from your financial institution asking you to log in urgently, as there was an unauthorized login on your account. The email contains a link to enter your credentials.

Answer: It's a scam. This email sounds pretty PHISHy to us! Your financial institution would never pressure you to sign in with a link.

Question 2: Someone calls you claiming to be from your financial institution. They say they need to discuss activity on your account, but first, they need your name, mailing address and account number to verify your identity.

Answer: We smell a scam! If you receive a call like this, hang up and call your financial institution. Be sure to look up a known phone number and not just redial the number who called you.

Question 3: A text comes through on your phone stating that your financial institution needs to verify your information or your account will be closed within 24 hours. Just click the provided link and log in, or you could face potential account termination.

Answer: Definitely a scam! Financial institutions rarely—if ever—send links via text, nor will they use scare tactics. To verify the message, call your local branch or the number on the back of your card.

Get tricked by one of the scenarios? Up your fraud-fighting knowledge by:

- **Visiting** BanksNeverAskThat.com and reading through their information and resources, taking quizzes, playing Scam City and more.
- **Watching EPCOR's fraud-fighting *Did You Know* videos**, available on YouTube, LinkedIn and EPCOR's website.
- Taking advantage of the Consumer Financial Protection Bureau's fraud and scam resources.
- Staying tuned to Fraud.org's fraud alerts.

Source: BanksNeverAskThat.com

Electronic Payments Core of Knowledge

EPCOR is a not-for-profit payments association which provides payments expertise through education, advice and member representation. EPCOR assists banks, credit unions, thrifts and affiliated organizations in maintaining compliance, reducing risk and enhancing the overall operational efficiency of the payment systems. Through our affiliation with industry partners and other associations, EPCOR fosters and promotes improvement of the payments systems which are in the best interest of our members.
For more information on EPCOR, visit www.epcor.org.

Nacha® Direct Member

The Nacha Direct Member mark signifies that through their individual direct memberships in Nacha, Payments Associations are specially recognized and licensed providers of ACH education, publications and advocacy.

www.epcor.org
2345 Grand Blvd., Ste. 1700, Kansas City, MO 64108
800.500.0100 | 816.474.5630 | fax: 816.471.7665