IEC Cybersecurity Presentation
October 4, 2018
3:00 PM to 4:30 PM
IECRM Offices

"Knowledge is power".
Francis Bacon - 1583

"Identity Theft" facts: (ID Theft Resource Center)

- 2005 -2018: 9,395 breaches
- 1,115,562,716 people exposed
- 50 per minute
- 3 years to recovery
- 25 people you know affected

What is "Identity Theft"

Identity theft is the crime of using another person's personal information, credit history or other identifying characteristics in order to make purchases or borrow money without that person's permission.

What Do Thieves Do with your Information?

Once identity thieves have your personal information, they can drain your bank account, run up charges on your credit cards, open new utility accounts, or get medical treatment on your health insurance. An identity thief can file a tax refund in your name and get your refund. In some extreme cases, a thief might even give your name to the police during an arrest.

Warning Signs of "Identity Theft"

- You see withdrawals from your bank account that you can't explain.
- You don't get your bills or other mail.
- Merchants refuse your checks.
- Debt collectors call you about debts that aren't yours.
- You find unfamiliar accounts or charges on your credit report.
- Medical providers bill you for services you didn't use.
- Your health plan rejects your legitimate medical claim because the records show you've reached your benefits limit.
- A health plan won't cover you because your medical records show a condition you don't have.
- The IRS notifies you that more than one tax return was filed in your name, or that you have income from an employer you don't work for.
- You get notice that your information was compromised by a data breach at a company where you do business or have an account.

What to do when your identity is stolen

Contact one of the credit reporting agencies' fraud alert departments and place a fraud alert on your credit report. This prevents identity thieves from opening accounts in your name. Many credit card

companies offer no-cost fraud protection where you would not be held financially responsible for charges made to your account by thieves who steal your personal information. In order to receive the most protection possible, though, it is important you call one of the credit reporting agencies as soon as you possibly can, even if you aren't 100 percent sure your identity has been stolen, but may only think it has.

Tell the agency you think your identity has been stolen. The agency will ask you to verify your identity with your Social Security number, name, address, and possibly other personal information.

One call does it all. The credit reporting agency you contacted must contact the other two. Each agency will place a fraud alert on their version of your credit report. For the next 90 days, your creditors and other businesses that want to offer you credits will see the alert on your credit report. If anyone asks for credit in your name, the appropriate lender will contact you to verify your identity and find out if you asked for credit.

FTC

Equifax Fraud Department
Call 1-800-525-6285
Visit www.equifax.com

Experian Fraud Department
Call 1-888-397-3742
Visit www.experian.com

TransUnion Fraud Department
Call 1-800-680-7289
Visit www.transunion.com

1. **Contact your lenders, banks, and insurance companies** and let them know the situation. Ask to close accounts. Open new ones with new personal identification numbers (PINs) and passwords.

2. **Victims of identity theft are entitled to a free credit report**. Wait about a month before you request it. Some activity may take a while to show up on your report. When you get it look for:

    - Personal information that has changed: your name, date of birth, Social Security number, address, and employer
    - Inquiries from companies you didn't contact
    - Accounts you didn't open
    - Debts on your accounts you can't explain

3. **File a police report—it is proof of the crime**. If the credit reporting agencies need to investigate fraudulent activity on your report, they will need this police report.

4. **Periodically check your credit reports** over the next year to make sure no new fraudulent activity has occurred.

5. **Work with the credit reporting agencies** to remove fraudulent activities from your credit report.

6. **Work with your credit card companies** to reverse fraudulent charges to your credit card.

How to recover from "Identity Theft"

1. Replace missing documents
2. File an "Identity Theft" report. FTC report & Police Report
3. Create an initial fraud alert and order your credit reports.
4. Request an extended fraud alert
5. Create a credit freeze
6. Act quickly if you think medical "Identity Theft"
7. Clear compromised tax records
8. Dispute fraudulent activity on financial accounts
9. Monitor your identity for the future

Agencies to Work with "Identity Theft"

1. Federal Trade Commission
2. State Attorney General
3. Local Police Departments
4. Your ID Theft Protection Provider

For more information contact
The Kyle Group
1410 Grant Street
Suite B302
Denver, Colorado 80203
Cell: 303-263-5422
Email: Ckyle@TheKyleGroup.com