ID Monitoring | iLOCK360

Why is identity monitoring so important?

Identity theft has lasting effects. Both financially and socially.

- Professional reputation
- Personal reputation
- Job Applications
- Lost Opportunities
- Travel

What Should I Be Looking for?

Outline

- ❑ Changes in Court Records
- ❑ Applications for Credit
- ❑ Use of your SSN
- ❑ Stolen usernames
- ❑ Stolen passwords
- ❑ Other unusual activity

What can I do?

Outline

- ❑ Password Management
- ❑ Financial Accounts
- ❑ Mobile
- ❑ Email
- ❑ Obtain Identity Monitoring Service

Password Management

Managing passwords properly is a huge pain. However it is very much within our control and extremely effective at keeping your digital assets safe. The importance of this cannot be overstated.

- Research indicates that 59% of the populations continues to use the same password for multiple accounts
- Countless accounts are breached as a result of old, stolen login credentials to access other accounts
- Unfortunately it still takes about 191 days for organizations to identify a breach

Suggestions:

- Don't reuse or recycle passwords
- Use a Password Manager

Source: Forbes - Why Reused Passwords Could Put Your Tax Information At Risk

Financial Accounts

You want to protect the accounts where you have your hard earned money. Don't forget to protect the digital assets that affect how you can make or borrow money in the future as well.

Vulnerable Targets

- Applications for Credit
- Tax fraud
- Children's Identities
- Phone & Internet scams on seniors

Suggestions

- If not applying for credit, freeze your credit account
- Monitor your children's credit reports to check for identity theft as often as your own

Mobile

Your mobile device knows almost everything about you. Where you live, where you work, who you talk to, where bank, and so much more.

Suggestions:

- Be careful with free Wi-Fi
- Don't put random apps on your phone
- Don't open or click on links sent by unknown contact
- Phone password
- Turn off your Bluetooth service when you aren't using it
- Use a protected app to store pin numbers and credit cards

Source: www. Engadget.com

Email

Website and application security along with encryption really do work well. It turns out fooling people into giving up their passwords is much easier than cracking their systems, and 75% of all attacked business reported fraudulent emails (Cyber Security Breaches Survey 2018).

Suggestions:

- Add Multi factor authentication
- Do not open emails from unknown senders or click links
- Protect email with encryption

Identity Monitoring Service

Too much of your information is already out there and simply trying to keep up with the latest news will not be enough. Most data breaches are already old by the time the public is made aware. Taking action quickly will eliminate the risk from most exposures.

Suggestions

- Have a process for reviewing alerts
- Take swift action to protect accounts
- Dispute discrepancies

Source: www. Engadget.com

What can we expect in the next few years?

Growing Threat

In the next year, the Identity Theft Resource Center predicts identity theft protection services will primarily focus on data breaches, data abuse and data privacy

Cybercriminals attack Internet of Things devices an average of 5,233 times per month.

The number of account takeovers also increased, rising from 380,000 in 2017 to 679,000 in 2018. Both individuals and enterprises are at risk for account takeovers

Internet Of Things

Internet of Things is the network of wirelessly connected devices

- This way hackers can gain control of important devices in your home

Suggestions

- Keep security software up to date
- Use different and difficult passwords
- Keep your mobile device on you at all times
- Tech recycle

More Phishing and Spear Phishing

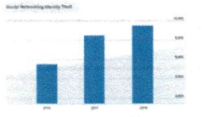
System security is becoming better and more accessible for organizations of all sizes and awareness is no longer a problem. Social engineering will continue to be the most effective angle.

- Business email compromises
- Voice replication technology
- Exploitation of company procedures
- Hacking system to system integrations

Social Media

Social Media and Networking Sites are gold mines for cybercriminals who can I discover a person's name, date of birth, phone number, hometown and other sensitive information relatively easy

- Last year, the FTC processed 9,439 email or social media identity theft reports, a 23% increase from 2017.



Source: Consumer Affairs - 2020 Identity Theft Statistics

Synthetic Fraud

Synthetic identity theft often includes a combination of fake and real credentials using names, Social Security numbers, driver's licenses and employee identification numbers to create new "synthetic" or fake identities

- Since synthetic identity theft and fraud uses only some of your actual personal credentials, the fraud does not always show up on your credit-bureau report
- Synthetic identity theft and fraud is problematic for the credit bureaus to detect, as the information is not an exact match, this it is difficult to reconcile

Source: Identity Theft Resource Center

Questions?

THANK YOU!

RESOURCES:

Go to https://www.ilock360.com/blog/ to for more education on cyber threats as well as tips to avoid becoming a victim of identity fraud. We have created seasonal content that is accessible on our website to help bring awareness.