January 2016
Volume 11, Issue 1

The Hidden Costs of a Data Breach

United Republic Bank
You and URB.

From the Desk of Thomas F. Duffy, Chair, MS-ISAC

A data breach is the intentional or unintentional release of information into an untrusted environment. Occasionally the release is accidental, but sometimes malicious actors specifically target retail stores, healthcare companies, or government agencies for the express purpose of gaining access to protected information, which they can use for financial gain. Sometimes they post the information they steal on the Internet or sell it in the cyber underground. Credit card numbers and personally identifiable information (PII) are prominent targets in these thefts, but malicious actors also want access to protected health information (PHI), online accounts, and information that can be used in tax and other fraud.

Identity Theft and Identity Fraud

Data breaches commonly lead to identity theft and identity fraud because malicious actors can gain easy access to large amounts of data, including names, addresses, dates of birth, and Social Security Numbers. This data allows the malicious actors to open bank accounts, credit cards, and other lines of credit in the victim's name.

According to the Department of Justice, identity theft and identity fraud are crimes in which someone wrongfully obtains and uses another person's personal data in some way that involves fraud or deception.

Tax Fraud

A variation of identity fraud occurs when the victim's information is used to file fraudulent tax forms. Some variants of tax fraud occur when fraudulent tax returns are filed in the victim's name while other variants occur when the malicious actors call the victim and pretend to be Internal Revenue Service (IRS) agents. In the first instance, the information from a data breach is used to fill out the tax forms, and in the second instance, the information is used to convince the victim that the malicious actor works for the IRS and has access to the victim's tax forms.

Medical Fraud

While more rare, medical identity theft is a growing concern because malicious actors use the victim's PHI to gain fraudulent access to medical care, surgery, and prescription drugs to

perpetrate additional fraud or resell on the black market.

Online Account Access

According to a TrendMicro report,[1] access into online accounts are in many cases more valuable than other identifying information, and can cost $1-15 per account. This is because malicious actors can use stolen accounts to gain access to additional information, as well as the services those accounts offer, such as additional purchases and streaming videos or music. For this reason, data breaches exposing online account information are increasingly common.

Telephone Scams

Scammers who operate over the telephone often use information obtained from other sources, including data breaches, to sound more authoritative. A recent variation on the Tech Support Call Scam involves just this type of activity with the callers using information from a data breach to help them pretend to be from a company that the victim had contacted for support.

Recommendations

If you believe you are the victim of identity theft or fraud, there are a couple of steps you should take:

1. File a report with your local law enforcement agency.
2. File a report with the Federal Trade Commission (FTC) at www.identitytheft.gov.
3. File a report with the three major credit bureaus and request a "fraud alert" for your account (Equifax – www.equifax.com, Experian – www.experian.com, TransUnion – www.transunion.com).

Further Information

- Tax scam information from the IRS: https://www.irs.gov/uac/Tax-Scams-Consumer-Alerts
- Security Awareness for Tax Payers by the IRS: https://www.irs.gov/pub/irs-pdf/p4524.pdf
- Identity Theft and Fraud information from the FTC: https://www.identitytheft.gov/
- Medical Identity Theft information from the FTC: https://www.ftc.gov/tips-advice/business-center/guidance/medical-identity-theft-faqs-health-care-providers-health-plans

Provided By:

MS-ISAC MULTI-STATE Information Sharing & Analysis Center™

STOP | THINK CONNECT™

---

[1] TrendMicro. North American Underground: The Glass Tank. http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-north-american-underground.pdf