Recognizing and Avoiding Online Scams

According to the Identity Theft Resource Center, the annual number of records exposed rose 126% in 2018, even while the annual number of data breaches fell by 23%. The business sector experienced 46% of the data breaches in 2018, followed by the medical and health care sector at 29%.[1]

This crime occurs when a thief obtains confidential information -- including passwords, personal ID numbers, Social Security numbers, or an account number used with a financial institution -- and uses it to commit fraud. Identity thieves use a victim's stolen information to open bank and brokerage accounts, run up bills for credit card purchases, obtain loans, and commit other forms of financial fraud.

Criminals obtain a victim's personal information in a number of ways -- both online and off. But as incidents of identity theft grows, so too does the arsenal of tools and sophistication level of techniques used to perpetrate the crimes.

Cybercrime: A Rapidly Shifting Model

Although online crime is a fast-moving target, currently, the primary methods in use by identity thieves are social engineering and phishing -- or typically a combination of both.

As the term implies, social engineering relies heavily on human interaction and often involves tricking unsuspecting victims into breaking normal security procedures. In short, it is a way for criminals to gain access to your computer or mobile device and the sensitive personal data it stores. For instance, a social engineer may use text messaging to contact a mobile device inviting the user to click on a link to a bogus website where the thieves collect user credentials and other personal information.

Similar results can be achieved through a phishing attack, in which the criminal uses email to lure victims to fake websites and then gain access to their passwords and usernames, credit card numbers, and other key data. Phishing emails often appear to be from a legitimate company that the victim recognizes.

In yet another instance, attackers may inject infected "malicious" code onto your computer via email attachments, links contained in emails, infected search engine results, or through videos and documents on legitimate websites, particularly social networking sites. In the mobile device world, criminals can corrupt a legitimate smartphone app and upload it to a third-party site. If users innocently install the app, they expose their devices to assaults by hackers who collect personal user data, change device settings, and sometimes even control the device remotely.

Don't Be a Victim

In today's 24/7/365 world, it is nearly impossible to secure all sources of personal information that may be "out there" waiting to be intercepted by eager thieves. But you can help minimize your risk of loss by following a few simple hints offered by the Federal Bureau of Investigation (FBI):

- Never divulge your credit card number or other personally identifying information over the Internet or telephone unless you initiate the communication.
- Reconcile your bank account monthly, and notify your bank of discrepancies immediately.
- Actively monitor your online accounts to detect suspicious activity. Report unauthorized financial transactions to your bank, credit card company, and the police as soon as you detect them.
- Review a copy of your credit report at least once each year. Notify the credit bureau in writing of any questionable entries and follow through until they are explained or removed.
- If your identity has been assumed, ask the credit bureau to add a statement to that effect to your credit report.
- If you know of anyone who receives mail from credit card companies or banks in the names of others, report it to local or federal law enforcement authorities.

Finally, be very wary of any email or text message expressing an urgent need for you to update your personal information, activate an account, or verify your identity. Practice similar caution with email attachments and downloadable files and keep your computers protected with the latest security updates and virus protection software.

Source/Disclaimer:

[1]Identity Theft Resource Center, 2018 End-of-Year Data Breach Report, 2019.

Required Attribution

Because of the possibility of human or mechanical error by DST Systems, Inc. or its sources, neither DST Systems, Inc. nor its sources guarantees the accuracy, adequacy, completeness or availability of any information and is not responsible for any errors or omissions or for the results obtained from the use of such information. In no event shall DST Systems, Inc. be liable for any indirect, special or consequential damages in connection with subscriber's or others' use of the content.