picture courtesy of digitaltrends.com

Tips from NY Regulators on Protecting Data

By: Patty P. Tehrani, Founder Policy Patty Toolkit (www.policypatty.com)

Date: February 1, 2018

Published on LinkedIn:
https://www.linkedin.com/pulse/tips-from-ny-regulators-protecting-data-patty-tehrani/

Did you see the helpful reminder from the New York State Office of Information and Technology Services and the Division of Consumer Protection issued to consumers and businesses to protect their online privacy and information from scams? If not, below is a summary as well as helpful resources from regulators that raise awareness of privacy and data security requirements and best practices. These measures are easy-to-follow and as the reminder provides to be done periodically to minimize risk and avoid becoming a victim of cyber-attack or data breach.

Summary

Keep personal information and data safe through the following recommended measures:

- Requests for Personal Information
    - Never share personal information, such as your Social Security number, in response to an unsolicited email or telephone call.
    - If the email or call claims to be from a company you do business with, call them first to confirm the contact is legitimate.
- Mobile Devices

- Apply software updates that patch known vulnerabilities as soon as they become available.
- Use security features built into your devices such as a passcode, and programs that encrypt data and remotely wipe contents if the device gets lost or stolen.

- Wi-Fi Hotspots
  - Public wireless hotspots are not secure, which means that anyone could potentially see what you are doing on your mobile device while you are connected.
  - Limit what you do on public Wi-Fi and avoid logging into sensitive accounts.
- Applications
  - Be sure to thoroughly review the details and specifications of an app before you download it.
  - Review and understand the privacy policy of each mobile app.
  - Be aware that the app may request access to your location and personal information.
- Information on Social Media
  - Avoid posting your birthdate, telephone number, home address, or images that identify your job or hobbies. This information may often reveal answers to security questions used to reset passwords, making you a possible target of scammers looking to access your accounts and secured information.
- Passwords
  - Create unique passwords for all your accounts. Use 10-12 characters in a combination of letters (upper and lower case), numbers and symbols.
  - Individuals should regularly change their passwords as well.
- Security Questions
  - Don't use the same security questions on multiple accounts. Be careful to select security questions for which only you know the answer.
  - Make sure the answers cannot be guessed or found by searching social media or the internet.
- Accessing Accounts
  - For additional security, require your password and an extra security code to verify your identity whenever you sign-in to your accounts, where available.
- Phishing

- Do not click on links, download files or open attachments in emails from unknown senders.
- Open attachments only when you are expecting them and know what they contain, even if you know the sender.
- And be wary of calls or texts asking for your personal information.

- Updates and Back-up Data
  - Make sure automatic updates are turned on for your software and that you back up all information.
- Financial Accounts
  - Review your bank, credit card, and account statements billing statements carefully to check for suspicious activity.
  - Report any suspicious charges immediately to the responsible financial institution.
- Credit Reports
  - If you identify inaccurate, suspicious or unusual activity on your consumer credit report notify the reporting consumer credit reporting agency and the respective financial entity immediately.
  - Consider placing a Security Freeze on their credit reports.
    - Experian: 1-888-397-3742
    - TransUnion: 1-800-680-7289
    - Equifax: 1-800-525-6285
- Records
  - Keep all notes and records about the security breach in the event fraudulent activity arises later.

You can read the full release here: http://www.dfs.ny.gov/about/press/pr1801261.htm.

Additional guidance, tips, and online safety resources, including real-time advisories:

- Visit the New York State Office of Information Technology Services website at **https://its.ny.gov/eiso**.
- For more information on security breaches and avoiding identity theft visit the Division of Consumer Protection website at **http://www.dos.ny.gov/consumerprotection/security_breach/**. Consumers may also contact the Division's Consumer Assistance Helpline at (800) 697-1220. Y
- Follow the Division of Consumer Protection on social media on Twitter (@NYSConsumer) and Facebook (**www.facebook.com/nysconsumer**).
- Check out the business center blog from the FTC: https://www.ftc.gov/tips-advice/business-center/privacy-and-security/consumer-privacy