Protecting your Personal Information

Cybersecurity risks such as identity theft, hacking and data breaches are rising in importance. Here are ten best practices from **GSAM's Strategic Advisory Solutions**.

1. Even seemingly unimportant accounts can introduce risk. Creating a unique password for every online account can help mitigate risk.

2. Strong passwords are typically 15 or more characters in length, are randomly generated and include a combination of upper and lower case letters, numbers and symbols.

3. Monitoring bank, credit card, and investment statements regularly can help spot unusual activity. The same is true of ordering a credit report at least annually.

4. Free Wi-Fi at coffee shops, hotels, airports and other public places is typically unsecured. Checking email and financial accounts from public computers, may increase risk.

5. Smart TVs, gaming consoles and wireless routers may have privacy settings and default passwords. Changing defaults regularly can help mitigate risk.

6. Giving away personal information in the naming of home wireless networks links the network to a specific location, and thus may invite hacking attempts.

7. Creating a few different email accounts can help mitigate risk, especially a separate account for banking and financial transactions.

8. When answering an account's security questions, there is no need to provide real answers. Making up answers and storing them in a password manager potentially can help reduce risk.

9. Cellular accounts have PIN codes -- they can be used in the effort to prevent unauthorized access.

10. Carrying out financial activities on one device and another to surf the web or access e-mail can help isolate sensitive accounts.

Important Disclosures

This presentation is intended to provide a general overview of some of the most common, current measures frequently taken to address cyber-security risk. The cyber security risk landscape is constantly evolving and the information security measures needed to respond to those risks will naturally change over time and differ from one individual to another. As a result, you are strongly advised to stay abreast of developments in cyber security and to consult your own information security and technical experts. Goldman Sachs does not represent that this document will be appropriate or adequate for your intended purposes.

This material is provided for informational purposes only. It is not an offer or solicitation to buy or sell any securities.

THIS MATERIAL DOES NOT CONSTITUTE AN OFFER OR SOLICITATION IN ANY JURISDICTION WHERE OR TO ANY PERSON TO WHOM IT WOULD BE UNAUTHORIZED OR UNLAWFUL TO DO SO.

Views and opinions are current as of the date of this presentation and may be subject to change, they should not be construed as investment advice. Although certain information has been obtained from sources believed to be reliable, we do not guarantee its accuracy, completeness or fairness. We have relied upon and assumed without independent verification, the accuracy and completeness of all information available from public sources.

Views are as of January 15, 2015 and subject to change in the future.

Goldman Sachs does not provide legal, tax or accounting advice to its clients. All investors are strongly urged to consult with their legal, tax, or accounting advisors regarding any potential transactions or investments. There is no assurance that the tax status or treatment of a proposed transaction or investment will continue in the future. Tax treatment or status may be changed by law or government action in the future or on a retroactive basis.

Confidentiality

No part of this material may, without GSAM's prior written consent, be (i) copied, photocopied or duplicated in any form, by any means, or (ii) distributed to any person that is not an employee, officer, director, or authorized agent of the recipient