

# Cybersecurity in a digital and interconnected world

## Workshop Checklist

### PROTECTING YOURSELF IN A DIGITAL AND INTERCONNECTED WORLD

No one is immune to cyber risk, but there are steps you can take to educate yourself and help minimize the odds of an incident.

#### Be Aware: Know These Threats

##### Viruses



Viruses are pieces of malicious code that install themselves and run without permission on a computer or mobile device.

##### Social Engineering



Social Engineering is when criminals pretend to be people they are not in order to deceive you into divulging confidential information.

##### Phishing



Phishing is the practice of using e-mail to lure the recipient to divulge personal information by clicking a malicious link or open an attachment.

##### Identity Theft



Identity theft is the fraudulent acquisition and use of a person's private identifying information, usually for financial gain.

#### Protect: And Understand

##### PASSWORD SECURITY

- Use a combo of special characters, upper and lower case letters, numbers, and 8+ characters
- Ensure it cannot be found in a dictionary
- To help remember, use a phrase ("I\_luvCA1n06") or use Password Manager software
- Do not share it with others, use across sites, or write it down
- Use two-factor verification for email
- Reset passwords at least 2 times a year

##### SEARCH ENGINES & ONLINE SHOPPING

- Only shop with reputable vendors
- Do not provide unnecessary personal information
- Only use credit cards or PayPal for online purchases
- Do not use debit cards online

##### SOCIAL NETWORKS

- Review privacy settings regularly
- Connect only with people you know; follow entities or public figures, don't "friend" them
- Do not post photos or information you would not want public
- Build groups (real friends, family, acquaintances); selectively post information to appropriate groups.

##### DATA PROTECTION

- Encrypt sensitive communications
- Encrypt data stored on personal computers
- Lock computer or logout when away
- Avoid using public computers or Wi-Fi hotspots to send personal information
- Backup data to a secure offline location
- Do not store/send sensitive data on email or Text

## PROTECT YOUR PORTABLE DEVICES

- Create a security PIN for your cellular account
- Set a screen lock password, screen lock your device after one minute of inactivity
- Do not allow text messages or caller ID to appear on your locked screen
- Turn off location services for unnecessary apps
- Always install software updates or subscribe to automatic ones
- Change default passwords (e.g. Bluetooth devices)
- Avoid using “jail-broken” or “rooted” devices

## IF YOUR EMAIL IS COMPROMISED

- Change your password immediately
- Review your settings for “reply to” or “forwarding” rules for tampering
- Immediately stop using the account for ‘authentication’ messages and financial transactions
- Do not use email to send or store personal information (government identification numbers, tax returns, etc.), unless encrypted

## IF YOUR IDENTITY IS STOLEN

- Review bank accounts, credit cards, web sites, tax returns; close unauthorized accounts
- Reset all passwords
- Place alert notices on financial accounts and with credit bureaus
- Consider ID Theft protection or credit monitoring services
- Review the **FTC Checklist** for step by step guidance on actions to take (see the footnote for more information)

## IF FRAUDULENT TRANSACTIONS APPEAR ON YOUR BANK ACCOUNT

- Contact your bank and financial providers immediately to place notices on your accounts
- Review recent account activity for all your accounts; report suspicious activity or transactions
- Consider ID Theft protection or credit monitoring services
- Replace your credit cards
- Ask your bank to issue new bank account numbers and checks



**Strategic Advisory Solutions** provides a comprehensive suite of integrated solutions designed to help our clients grow and enhance their businesses. Our global team of experienced strategists aims to deliver in-depth expertise to help clients understand dynamic markets, design well-diversified strategic portfolios, and implement industry best practices through programs tailored to each organization. We partner with our clients to develop actionable solutions to help them achieve their goals.

For more information, contact us at [StrategicAdvisorySolutions@gs.com](mailto:StrategicAdvisorySolutions@gs.com) or visit us on the web at [www.gsamfunds.com](http://www.gsamfunds.com).

Sources: The US Federal Trade Commission (FTC) gives guidance for preventing and responding to identity theft at: [www.onguardonline.gov](http://www.onguardonline.gov) and [www.consumer.ftc.gov/features/feature-0014-identity-theft](http://www.consumer.ftc.gov/features/feature-0014-identity-theft). Cybersecurity Guidance provided by GS Technology Risk; United States Computer Emergency Readiness Team – Security Tips (ST04-002) - Choosing and Protecting Passwords; Federal Bureau of Investigation (FBI), Internet Social Networking Risks website.

The website links provided are for your convenience only and are not an endorsement or recommendation by GSAM of any of these websites or the products or services offered. GSAM is not responsible for the accuracy and validity of the content of these websites.

This presentation is intended to provide a general overview of some of the most common, current cybersecurity threats, and the measures frequently taken to address them. Although these steps are important for keeping online identities safe, it is not a guarantee and additional steps may be necessary. The cybersecurity 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 client to another. As a result, you are strongly advised to stay abreast of developments in cybersecurity 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 educational purposes only and should not be construed as investment advice or an offer or solicitation to buy or sell securities. Views and opinions expressed are current opinions as of the date appearing in this material only. **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.

© 2015 Goldman Sachs. All rights reserved. Date of First Use: October 5, 2015. 170432.OTHER.MED.TMPL/10/2015