YOUR PERSONAL INFORMATION: PROTECTING IT FROM EXPLOITATION

Data breaches involving personal information result in a broad range of risks to individuals and organizations. This includes identity theft, targeting of individuals with knowledge of sensitive government information and internal business processes, and other intelligence activities that use personal information of U.S. citizens to undermine national security.

It is in our collective interest that we take actions to limit the risk of our personal information being exploited, and that we are able to recognize any indicators that we may be the target of such activities.

Confirmation that your personal information has been accessed in a data breach is not a guarantee that your information will be misused or that you will be targeted for further exploitation. However, it is important to remain mindful of the risk of such misuse or exploitation. The following information is provided to raise your awareness to this possibility and to help you understand how your personal information may be used by foreign intelligence services, and other "bad actors" (extremists, criminals, hackers, and the like).

The information below is provided to raise awareness and provide guidance for mitigating risks; it is not intended to indicate that the government has observed particular adverse effects from data compromises.

GENERAL AWARENESS AND PROTECTION GUIDANCE

All individuals potentially affected by a breach should be wary of suspicious activities indicating their personal information has been or is being exploited, and follow these protective measures, including:

- *Do not provide additional or detailed information about yourself, your family or associates, or your position with any individual who has an unusual or heightened interest in you, or your family and associates;*
- *Do not share personal, financial, or sensitive information if you are contacted by unknown individuals or groups via e-mail, instant messaging or text, telephone, social media interaction, and personal encounters;*
- *Do not open attachments or click on links embedded in emails, instant messages or texts from unknown senders, senders who would be unlikely to send an email directly to you, and even from known senders with grammatical errors, misspellings, or if there is no text with the attachment or link;*
- *Install and maintain up-to-date anti-virus and anti-malware software to guard against viruses, other malicious code, and pop-ups that can appear if your computer is infected;*
- *Transmit electronic information safely using encryption and by using secure, known websites (e.g., with addresses starting with "https" rather than "http");*
- *Share electronic files and photographs only with those you know as they contain embedded metadata such as identity, date and time, and location information;*
- *Select the highest level of privacy settings on your electronic devices and applications;*
- *Monitor your credit history and activity through a reputable credit bureau and your account statements for any unauthorized or unusual entries. Free credit reports can be obtained at:* ***http://www.consumer.ftc.gov/articles/0155-free-credit-reports****;*
- *Maintain direct positive control of, or leave at home, electronic devices during travel, especially when traveling out of the U.S.;*
- *Know the locations and contact information for U.S. embassies, consulates, and other diplomatic establishments for any issues or emergencies when*

Continued on Page 2.

REPORTING

To protect yourself and your family, we urge all affected individuals to exercise caution and remain vigilant to any events appearing out of the ordinary or suspicious.

If you believe you have observed activity related to a personal data compromise or suspect your personal information has been exploited, report your concern promptly as instructed by your leadership.

The appropriate Federal government sites may also be used to report specific incidents:

- *Report any suspected instances of identity theft to the FBI's Internet Crime Complaint Center at* ***www.ic3.gov****.*
- *If you notice fraudulent activity, go to the Federal Trade Commission (FTC) website (www.ftc.gov/idtheft or www.identitytheft.gov) and complete an ID theft complaint form and place a fraud alert on your credit report.*
- *Report unexplained activity related to criminal behavior to the local police department. Provide them with a copy of the FTC form and request a copy of the police report.*

More Information:
Additional information can be found at the **ncsc.gov** web site, including:

- *Video Message from NCSC Deputy Director Dan Payne, Your Personal Information – Protecting it from Exploitation*
- *NCSC Overview Presentation, Your Personal Information – Protecting it from Exploitation*

Continued from Page 1.

traveling out of the country. This information can be found at: ***http://www.state.gov/misc/list/index.htm****;*

- *Report per your department, agency, or company instructions, all suspicious activity, events, or individuals you, relatives, and associates encounter; and*
- *Share these general awareness and protection guidelines with relatives and associates as appropriate. Avoid misconduct or behaviors that leave you vulnerable to blackmail, coercion, or recruitment.*

HOW YOU MIGHT BECOME A VICTIM

SOCIAL ENGINEERING is the term used to describe bad actors using information they have discovered either legally or illegally about you to gain your trust and extract further information or manipulate you to take actions you would not otherwise take.

The use of stolen personal information by cyber operators is highly valuable for social engineering as it can be used to create a compelling illusion that you already know an individual or have a shared interest with them. It opens a means to contact you in either cyber space or the physical world to foster that trust or do harm.

Examples of how bad actors may use your personal information for social engineering and other purposes include:

PHISHING (or spearphishing) is a common method used to contact people through email. With phishing, bad actors use social engineering to target their victims and lure them into taking actions that could ultimately compromise their computer or network. Examples include getting a victim to open a malicious attachment or clicking on a bogus embedded link. Like other social engineering attacks, spear phishing takes advantage of a victim's most basic human traits, such as a desire to be helpful, provide a positive response to those in authority, or respond positively to someone who shares similar tastes or views, or simple curiosity about contemporary news and events. Those who "take the bait," become unwitting participants in a computer network attack by allowing the attackers to bypass many of our technical defenses.
Phishing scams also trick you into providing your confidential information, which is then used to access your accounts. Typically this kind of fraud involves an email, text message, or pop-up window claiming to come from an official source.

SOCIAL MEDIA DECEPTION (including Facebook, Twitter, Google and LinkedIn) provides bad actors with an avenue to connect to their victims. Attackers may create a fake profile to befriend their victims while posing as a former acquaintance, job recruiter, or someone with a shared interest. Using a fake online persona, an attacker may try and get their victims to reveal more information about themselves or their employers, or they may simply collect more information about their victims from your social media postings.

HUMAN TARGETING is often used by foreign governments to target individuals with access to information of interest to them. For instance, you may unexpectedly meet someone at a venue of interest, such as a conference or child's school event, who shares your interests or views and establishes an ongoing relationship. Your new friend may test you by getting you to do seemingly small "favors" for them or getting you to talk about trivial work-related information. Over time, trivial information may lead them to information that is of interest.

TRAVEL VULNERABILITIES are greater than usual, especially if you are traveling outside of the U.S., as it is common for you to encounter unfamiliar people. Also, your guard may be down because you are traveling for vacation, training, or other relaxing purposes. Therefore, take extra precaution of:

- *Those who approach you in a friendly manner and seem to have a lot in common with you--especially if they wish to maintain contact with you once you return home.*
- *Interactions in social settings where you find you are unusually successful in meeting and impressing others.*
- *A seemingly random and/or other foreign acquaintance who has heightened interest in your work or introduces you to a third party who then wants to continue to meet with you.*

UNSOLICITED TELEPHONE AND TEXT MESSAGES from toll-free numbers can be set up quickly and sometimes exist solely for the purpose of capturing your confidential information, often simply by playing a prerecorded message about your accounts being in trouble. The message prompts you to enter your 16-digit account number. This is followed by a request for your PIN and other personal information. Or you may receive a text message or a phone call with a prerecorded message that describes an urgent situation that requires immediate action. The message may say, "Your account has been blocked. Please call 800-123-4567 to unlock it." Before you realize you're being scammed, you've given enough information to duplicate your card and access your accounts.

IDENTITY IMPERSONATION is acquiring key pieces of your confidential information, such as your name, address, birthdate, Social Security number, and mother's maiden name, in order to commit fraud. Identity Impersonation can be used as a tactic for corporate exploitation via the newly acquired identity. With this information, an identity thief can take over your financial accounts; open new bank accounts; purchase automobiles; apply for loans, credit cards, and Social Security benefits; rent apartments; and establish services with utility and phone companies, all in your name.