PROTECTING YOUR INFORMATION

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

Acting in ways that limit the risk of personal information being exploited is in our collective interest. We all need to be able to recognize signs that we may be the target of exploitation activities.

Confirmation that your personal information has been accessed through a data breach is not a guarantee that it will be misused or that you will be targeted for exploitation. Even so, you would do well to guard against the risk of such misuse or exploitation. This brochure offers information on exploitation tactics to help you understand how your personal information may be used by both foreign intelligence services and other "bad actors" (extremists, criminals, hackers, and the like).

REPORTING AND ADDITIONAL RESOURCES

To protect yourself and your family, we urge you to exercise caution and remain vigilant, noting any events that appear suspicious or out of the ordinary.

Report your concerns if you believe you have seen activity related to compromised personal data or if you suspect someone is exploiting your personal information.

You can also use the following federal government sites to report specific incidents. Report —

- Suspected identity theft to the FBI's Internet Crime Complaint Center at www.ic3.gov.
- Fraudulent activity on your account to the Federal Trade Commission (FTC) at www.ftc.gov/idtheft or www.identitytheft.gov. Complete an ID theft complaint form and place a fraud alert on your credit report.
- Unexplained activity or criminal behavior to your local police department. Give them a copy of the FTC form and ask for a copy of their police report.

NATIONAL COUNTERINTELLIGENCE AND SECURITY CENTER
NCSC
UNITED STATES OF AMERICA

Know the Risk
Raise your Shield

Additional information can be found at the ncsc.gov website.

NATIONAL COUNTERINTELLIGENCE AND SECURITY CENTER
NCSC
UNITED STATES OF AMERICA

Know the Risk
Raise your Shield

YOUR PERSONAL INFORMATION: PROTECTING IT FROM EXPLOITATION

An Informational Guide for Your
AWARENESS & PROTECTION

Know the Risk... Raise your Shield

Once personal information is compromised, it can be used by foreign intelligence entities, transnational criminal groups, and others to gain your trust and elicit more information. Victims of compromised personal data should be aware of the following commonly-used deception tools and techniques employed by our adversaries:

SPEAR PHISHING

Spear phishing is a common method bad actors use to attack people through email. They use your stolen personal information to create seemingly real and plausible or official emails, text messages, or pop-up windows to lure you into taking actions that could ultimately compromise your computer or network. Examples include urging you to open a malicious attachment or click on a bogus embedded link. Doing so could make you an unwitting participant in a computer network attack by allowing the attackers to bypass the network's technical defenses.

Spear phishing scams can also trick you into providing your confidential information, which the actors then use to access your accounts.

SOCIAL MEDIA DECEPTION

Social media (including Facebook, Twitter, Google, Instagram, and LinkedIn) gives bad actors a way to connect with their victims. Attackers may create a fake profile to befriend you, posing as a former acquaintance, a job recruiter, or someone with a shared interest. Using fake online personas, attackers may deceive victims into revealing more information about themselves or their employers or they simply collect more information about their victims from social media postings.

HUMAN TARGETING

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

SOCIAL ENGINEERING

When bad actors use information they have discovered about you — legally or illegally — to gain your trust, they can get more from you or manipulate you to take actions you would not otherwise take. For example, these actors use stolen personal information to create a compelling illusion that you are already acquainted or have a shared interest. This gives them a way to contact you, in whatever way, to foster that trust or do harm. They take advantage of a person's most basic human traits, such as a desire to help, respond to those in authority, respond positively to someone with similar tastes or views, or to satisfy simple curiosity about news and events.

TRAVEL AWARENESS

Vulnerabilities are greater than usual, especially if you are traveling outside of the United States, where you commonly encounter unfamiliar people. Also, your guard may be down because you are traveling for training, vacation, or other relaxing purposes. Therefore, take extra precaution with:

- Those who approach you in a friendly manner and seem to have a lot in common with you, especially if they wish to remain in contact 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 foreign acquaintance with heightened interest in your work or who introduces you to a third party who wants to continue to meet with you.

GENERAL AWARENESS AND PROTECTION GUIDANCE

All individuals potentially affected by a data breach should follow these measures to protect their information:

- ☑ Do not provide information about yourself, your family, your associates, or your position to any individual with an unusual or heightened interest.
- ☑ Do not share personal, financial, or sensitive information if contacted by unknown individuals or groups, in person or via email, instant message, text, telephone, or social media interaction.
- ☑ Do not open attachments or click on links embedded in emails, instant messages, or texts from unknown senders, those unlikely to email you directly, or from senders you know if the message has errors in grammar or spelling, or if no text accompanies it.
- ☑ Always install and maintain up-to-date anti-virus and anti-malware software to guard against malicious code.
- ☑ Send electronic information safely by using encryption and secure, known websites (e.g., those starting with "https").
- ☑ Apply the highest privacy settings available on your electronic devices, applications, and social media accounts.
- ☑ Monitor your credit history and activity through a reputable credit bureau and your accounts for unauthorized or unusual entries. Go to: http://www.consumer.ftc.gov/articles/0155-free-credit-reports for a free credit report.
- ☑ When traveling, maintain direct control of your electronic devices or leave them at home — especially when traveling outside the United States.
- ☑ Avoid behaviors that leave you vulnerable to blackmail, coercion, or recruitment.