Pinellas County IG Working to Receive 2nd Statewide Reaccreditation

Pinellas County Clerk of the Circuit Court and Comptroller, Division of Inspector General (Pinellas County IG), is undergoing its 2nd Commission for Florida Law Enforcement Accreditation (CFA) assessment to retain its state level reaccreditation. The Pinellas County IG became the first local government agency in the nation and first Florida Clerk of the Court and Comptroller’s office to be awarded the status as an Accredited Office of Inspector General by the CFA on February 3, 2010 and achieved their first reaccreditation on February 21, 2013.

The CFA Assessment Team conducted the formal assessment on December 2, 2015 to examine all aspects of the Pinellas County IG’s Investigations Section, including policies, procedures, management, operations and support services. The Assessment Team has reported back to the full Commission for Florida Law Enforcement Accreditation, Inc., which will then decide if the Pinellas County IG is to receive its 2nd re-accredited status. Reaccreditation occurs every three years.

The examination is part of a voluntary process to gain reaccreditation, which is a highly prized recognition for Offices of Inspector General professional excellence. The assessment team is composed of investigators from other Florida Offices of Inspector General. The CFA reaccreditation process consists of assessing the IG agency on 44 standards. In order to earn reaccreditation by the CFA, the Pinellas County IG must comply with 42 of these standards, those which are applicable to areas of responsibility and jurisdiction. The assessors review written materials, interview individuals, and visit offices and other places where compliance can be witnessed.

Welcome to the IG Team:
Darcy Eckert, Inspector General Auditor I
Cassy Moreau, Inspector General Auditor I

Welcome Back:
Ava Jurek, Senior Inspector General Auditor

Promotions to Celebrate:
Melissa Dondero, Inspector General Manager
Anne DiNatale, Senior Inspector General Auditor
William McGuinness, Senior Inspector General Auditor
Deborah Weiss, Senior Inspector General Auditor
16 Ways You May Be Exposing Yourself to Fraud

Depending on what we do, and how we do it, those areas become bigger or smaller targets.

Here’s a list of ways we routinely expose more information than we may know to criminals. It happens every time you do one of the following things:

1. Pick up a phone, respond to a text, click on a link or carelessly provide personal information to someone we don’t know.
2. Fail to properly secure computers or mobile devices (smartphones, tablets or laptops).
3. Create easy-to-crack passwords.
4. Discard rather than shred a document that contains PII.
5. Respond to an email that directs us to call a number we can’t independently confirm, or complete an attached document that asks for PII in a non-secure environment.
6. Save our user ID or password for a website or app as a shortcut for future login.
7. Use the same user ID and password on different sites, whether for email, social, financial or school-related sites.
8. Take online quizzes that subtly ask for information we may have provided as the answers to security questions on secure sites.
9. Snap pictures with our smartphone or digital camera without disabling the geotagging function.
10. Fail to replace a manufacturer’s default password with a long and strong one of our own on any connected appliance or electronic device that we put in our homes.
11. Use our email address as a user name/ID, if we have the option to change it.
12. Use simple PINs like 1234 or 9876 or a birthday.
13. Forget to obtain, review and correct our credit reports.
14. Go 24 hours without reviewing our bank and credit card accounts to make absolutely sure that every transaction we see is familiar.
15. Fail to enroll in free transactional monitoring programs offered by banks, credit unions and credit card providers that notify us every time there is any activity on our accounts.
16. Use a free Wi-Fi network, without confirming it is correctly identified and secure, to check email or access financial services websites that contain our sensitive data.

In each of the above instances, we leave ourselves vulnerable to those who consider the theft of our identity as their day job. Learn more from Credit.com: How to Protect Yourself From Identity Theft

The above is an adapted excerpt from Swiped: How to Protect Yourself in a World Full of Scammers, Phishers and Identity Thieves.

“Scammers are all basically imposters,” notes Mary E. Power, president and CEO of the Council of Better Business Bureaus, the umbrella organization for 113 local, independent BBBs across the United States, Canada and Mexico. “Three of the top four scams reported to us are those that scare people with threats of arrest, law suits or other frightening actions. Scammers are pretending to be government agents, lawyers, debt collectors, police officers. They engage directly with you, so your best bet to avoid being scammed is to stop engaging. Hang up the phone, delete the email, shut the door.”

See more at: https://www.bbb.org/top10scams/