



Boise | Coeur d'Alene | Pocatello

PERSpectives FOR RETIREES

Public Employee Retirement System of Idaho

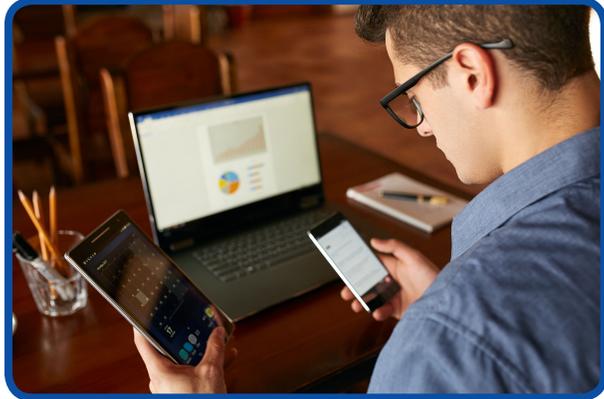
Third Quarter 2019

TOPICS / October Is National Cybersecurity Awareness Month – Keep Your Smart Devices Secure pg. 1-3 / Don't Get Left At The Gate! Make Sure You Are Ready To Fly With The Star Card! pg. 3 / Bulletins pg. 4 / Investment Report pg. 4

OCTOBER IS NATIONAL CYBERSECURITY AWARENESS MONTH – KEEP YOUR SMART DEVICES SECURE

Nowadays, nearly everyone has a smart device, especially a smart phone. While smart devices help us in a multitude of ways, they are also the fastest growing targets for criminals. Since we take our smart devices with us everywhere we go, they are more likely to be hacked, lost, or stolen than other devices we leave at home. More importantly, our devices are constantly exposed to other devices and networks.

Smart devices store so much of our personal information, and most of us have some type of app on our device. Depending on the app, it may provide access to our credit card data, bank accounts, or other kinds of sensitive information. Some of these apps may save our credit card information, allowing criminals to purchase whatever they want, and ship it to wherever they want.



Additionally for many of us, our smart device likely has direct access to our text messages, email, and social media accounts. In the wrong hands, our personal information can be used against us.

Sure, this can happen if our smart device is physically stolen, but there are a growing number of cases where devices are having their Wi-Fi, Bluetooth, and cellular connections compromised to gain access to our data.

Our smart devices can be infected with malware just like a computer can. Cybercriminals can steal our identity and impersonate us on social media. So what can we do to make sure our smart devices are secure and less susceptible? Here are some tips to help.

STRONG PASSWORD

Create a strong password for your smart device. Make it difficult for criminals, physical or cyber, to gain access to your sensitive information if they get access to your device.

continued on page 2...



...continued from page 1

FINGERPRINT LOGIN

If your smart device offers fingerprint login, seriously consider using it. You will add substantial security to your device by logging into your device with your finger or thumbprint. Fingerprints are much more complex than a password, and convenient since you can login with the touch of screen. Moreover, in case something happens to the scanner or your fingerprint, most devices require a backup password.

DISABLE WI-FI AND/OR BLUETOOTH WHEN YOU AREN'T USING THEM

Even if you are not using your Wi-Fi or Bluetooth connections, your phone is still broadcasting information and may be attempting to connect with other devices. This information can be used to track your location, and potentially gain access to your device.

If you are in a public place, like a movie theater, shopping center, or sporting event, a criminal can use these connections to tamper with your smart device and steal personal information or transfer malware.

Luckily, most smart devices make it easy to disable and enable wireless services, so you can prevent unwanted broadcasting.

BEWARE OF THE APPS YOU DOWNLOAD AND UNDERSTAND WHAT YOU LET THEM ACCESS

While companies try to inspect and screen the apps they offer, there are still apps that get through with malware that shares information to third parties. Download the wrong app, and you are more likely to be vulnerable to an attack.

Before downloading an app, do some research to make sure it is trustworthy. Avoid downloading apps that do not come from your device's official store. Equally important, delete apps that are no longer being used. They take up space on your device, and continue to gather data even if they aren't being used.

BE CAREFUL WHERE YOU CHARGE YOUR DEVICES

The power source you use to charge your smart device may do more than just power it up. It could also be a high-speed data link, meaning anything can be transmitted over that line. Your personal data could be extracted from your device or malware could be installed on your device. This kind of data extraction can happen quickly, without your permission, and without knowing it has happened until it is too late.

Avoid plugging your device directly into any USB socket found in a public place like a library, airport, or even a rental car. There is no way to know if the outlet has been tampered with. If you need to charge your smart device, use the adaptor and cable that came with the device and plug it into an electrical outlet, or use the USB port on your trusted computer/laptop. Most adapters cannot transfer or receive data to your device, only power.



continued on page 3...



...continued from page 2

KEEP YOUR DEVICES AND APPS UPDATED

The most important reason to keep your smart devices and apps up to date is security. With any software system or app, there are flaws that require tweaks, and it is just a matter of time before the bad guys discover the flaws and use them against you.

Companies like Google and Apple have employees whose job is to try to hack into their own products. They work to find and repair flaws before hackers can take advantage of them.

Fortunately, most smart devices and apps will notify you when an update is available, and prompt you with reminders.



ADDITIONAL RESOURCES AVAILABLE TO YOU

Learn more about smart device security and much more at:



Stay Safe Online (Powered by the National Cyber Security Alliance)

www.staysafeonline.org



U.S. Department of Homeland Security

www.dhs.gov

DON'T GET LEFT AT THE GATE! MAKE SURE YOU ARE READY TO FLY WITH THE STAR CARD!

We want to share important information with you from the Idaho Transportation Department about Star Card – Idaho's REAL ID.

Beginning Oct. 1, 2020, you will need a Star Card or a federally approved credential, such as a U.S. Passport, to board a flight or access a federal courthouse or military base.

Please plan ahead and consider getting a Star Card before the deadline.

To find out more about the deadline, requirements, and documents needed to obtain a Star Card visit this website: <https://itd.idaho.gov/starcard/> or call 208-334-8736.



You'll need a Star Card by **October 1, 2020**, to board a flight.



He's cleared for takeoff because he got a Star Card – Idaho's REAL ID.





**P.O. Box 83720
Boise, ID 83720-0078**

**PRSR STD
U.S. POSTAGE PAID
PERMIT NO. 829
BOISE, IDAHO**

BULLETIN • BULLETIN • BULLETIN • BULLETIN • BULLETIN • BULLETIN

DO YOU KNOW WHAT YOU CAN DO WITH *myPERSI*?

You can receive your PERSI annual statements, confirmations of changes, and other documents sooner and in a secure location by setting your preferred method of communication to electronic in your *myPERSI* account.



CLICK HERE

By choosing electronic communication, under the Personal Information tab on your *myPERSI* page, you will receive an email alert when new documents are available. Then you can log into your *myPERSI* account to download the documents.

PERSI INVESTMENT NEWS

AS OF August 29, 2019

VALUE OF THE FUND

\$18,407,276,301

FISCAL YEAR CHANGE IN MARKET VALUE

\$(112,131,753)

FISCAL YEAR-TO-DATE RETURNS: -0.3%

MONTH-TO-DATE RETURNS: -0.7%

*Posted monthly at www.persi.idaho.gov
Fiscal Year July 1, 2019 - June 30, 2020

RETIREMENT BOARD OF DIRECTORS

Jeff Cilek, *Chairman*

Joy Fisher, *Trustee*

Celia R. Gould, *Trustee*

Park Price, *Trustee*

Darin DeAngeli, *Trustee*

Executive Director • Donald Drum

Deputy Director • Michael L. Hampton

Public Information Officer • Jenny Flint

www.persi.idaho.gov

Costs associated with this publication are available from PERSI in accordance with Idaho Code 60-202.