THE SHIELD

MARCH 12, 2018

VOLUME II, ISSUE IV

The University of Texas Rio Grande Valley
Information Security Office

Take a Break!

This Spring, we hope that you can take a break and relax! Spring is the perfect season of the year to go through unfinished projects, do some spring cleaning, relax with friends and family, and eagerly await what summer will bring. For this issue, The Information Security Office (ISO) invites you to consider taking a few minutes to go through your computer assets, digital life, and give them a good rest too!
Please follow these tips that will guide you to refresh and renew your cyber life, and remember to share them with your friends and family:

Clean your devices:

- Smartphones, tablets, laptops, and computers require maintenance and spring cleaning is the perfect chance to do it! Delete unused applications or software and clear out any downloads you aren't using any more. Check for old files that can be archived or deleted. Make sure your device's security software is working properly and all software is patched and set to auto-update. We highly recommend that you **backup** your files and pictures before you update your computer!
- Last, but not least, take out the trash. Literally. Cross-cut shredders are the perfect choice when shredding sensitive papers! Additionally, there may be old devices in your house or office that could be recycled. All UTRGV computer hard drives must be removed and sanitized to ensure that any sensitive or confidential information it may contain is permanently erased and unrecoverable before the computer can be sent to surplus.

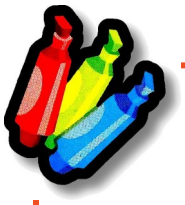
Clean your digital accounts:

- Email — Email accounts collect clutter and there may be information in your accounts that you can archive into folders or delete. A great idea is to set rules, by using rules you can reduce manual and repetitive actions, these can help you to stay organized. Do your best to empty your deleted items or trash folder on a regular basis.
- Social Media — Spring clean your social media accounts by following our "Don't get **SMACK**ed" campaign. Review the privacy and security settings on websites you use to ensure they're at your comfort level for sharing. It's OK to limit how and with whom you share information.

INSIDE THIS ISSUE:

Take a Break!	1
Security Highlights	2
EOL Softtware	3
Clean Desk Initiative	4
Data Privacy Day	5
SANS OUCH! March 2018	6

EDITOR
Francisco Tamez
Security Analyst



SECURITY HIGHLIGHTS

Critical flaws revealed to affect most Intel chips since 1995

On January 2018 security researchers have revealed the long-awaited details of two vulnerabilities in Intel processors dating back more than two decades. These two critical vulnerabilities found in Intel chips can let an attacker steal data from the memory of running apps, such as data from password managers, browsers, emails, and photos and documents.
The researchers who discovered the vulnerabilities, dubbed "Meltdown" and "Spectre," said that "almost every system," since 1995, including computers and phones, is affected by the bug.

Tax Season and Scams!
Here's how the Tax scam works: Cybercriminals use various spoofing techniques to disguise an email to make it appear as if it is from an organization executive. The email is sent to an employee in the payroll or human resources departments, requesting a list of all employees and their Forms W-2.
bit.ly/IRS-W2-alert

Feds charge 'Fruitfly' creator with hacking thousands of computers

The government claims, Phillip R. Durachinsky, 28, ran a 13-year scheme from 2003 to Jan. 20, 2017 that infected thousands of computers with malware dubbed "Fruitfly." Fruitfly, which targeted Mac computers, allowed Durachinsky to take complete control of a computer including secretly turning on cameras and microphones to record video and audio.

Are you a Phish?
Phishing is a form of fraud in which the cybercriminal tries to learn information by tricking you as a trustworthy entity or person via email, websites, and phone calls.

Things to look for in emails:

- Beware of links in emails! **NEVER** click them.
- **NEVER** download or open any attachments.
- **Hover** over links: Simply place your mouse over the link to see the web address. (Links might also lead you to .exe files. These kinds of file are known to spread malicious software.)
- Threats might be included. For example:
  - ◊ "Your account would be closed if you don't respond with your username and password."
- Scam artists use graphics in emails that appear to be connected to legitimate websites.

Social media and engineering used to spread Tempted Cedar Spyware

Cybercriminals are using social media and social engineering to dupe victims into downloading Advance Persistent Threat spyware disguised as the Kik messenger app.
The spyware dubbed "Tempted Cedar Spyware" is designed to steal information like contacts, call logs, SMS, and photos, as well as device information, like geolocation in order to track users and was capable of recording surrounding sounds, including conversations victims had while their phone was within range

Scam hijacks Google Chrome browser, tries to get your personal data

Scams that hijack the world's most popular browser, Google Chrome, are making the rounds again. It starts with a fake error message. For computer users, this is a vexing problem because the underlying malicious code locks up the browser. "The bug that it triggers is more than just an annoyance in the sense that it will render your Chrome browser unresponsive," Jerome Segura, Lead Intelligence Analyst at Malwarebytes, told Fox News.

These and more news can be found in: bit.ly/UTRGVisoNews

End Of Life Software

EOL Software
Software applications have a lifecycle. The lifecycle begins when the software is released and ends when it is no longer supported by the vendor, also called End Of Life (EOL). When software stops being supported by the vendor it can lead to no longer receiving security updates that can help protect your PC from harmful viruses, spyware, and other malicious software that can steal your personal information.
For example, Apple QuickTime 7 for Windows is no longer being supported.

EOL OS
Windows XP and Apple OSX 10.8 and below are EOL. If you are currently using an EOL Operating System (OS) you should upgrade your OS to maintain the security of your computer and data. Computers owned, leased or managed by UTRGV must adhere to the Computer Security Standard, (bit.ly/UTRUTRGVISOComputerSecurityStandard) which requires them to run only vendor supported OS.

Please update if you are using **previous** versions of any of the following products:

Supported products

Product	Version	Product	Version	Product	Version	Product	Version	Product	Version
Windows	7	OS X 10.11	El Capitan	Adobe Flash Player	26.0	Android	Jelly Bean	Java SE	8
Windows	8	OS X 10.12	Sierra	Adobe Reader	2017.012	iPhone	iOS 9.1	Internet Explorer	11
Windows	8.1	OS X 10.13	High Sierra	Adobe Acrobat X	2017.012			Google Chrome	60.2
Windows	10							Firefox	55.0.2

To successfully update to the latest OS you will need the following systems requirements. In the instance that the computer's hardware is not capable to stand the latest OS, then according to the computer security standard that computer will have to go through surplus and a new one with capable hardware will take its place.

If you use for your work activities a university owned computer with an Operating System with EOL, please log in to my.utrgv.edu and submit a ticket through Service Now or contact the IT Service Desk as soon as possible.

Brownsville / Harlingen / South Padre Island 956-882-2020

Edinburg / McAllen / Rio Grande City 956-665-2020

A friendly recommendation for students, faculty, and staff that use personal computers or laptops: Please review the following systems requirements, log in to my.utrgv.edu, visit the vSoftware application, and purchase ($9.95 USD) Windows 10; it is highly recommendable that you back up all of your files, photos, and any other important documents before you upgrade your OS. In the case that your personal computer does not support the OS, please consider upgrading your machine.

For more EOL software please visit: bit.ly/list-EOL2017

CLEAN DESK SECURITY BEST PRACTICE

An example of a BAD practice

A clean desk practice ensures that all sensitive/confidential materials are removed from an end user workspace and locked away when the items are not in use or an employee leaves his/her workstation. It is one of the top strategies to utilize when trying to reduce the risk of security breaches in the work-place. Please use the checklist below daily to ensure your work (or home) workspace is safe, secure, and compliant.

- ☐ Passwords should not be left written down in any accessible location.
- ☐ Ensure all sensitive/confidential information in hardcopy or electronic form is secure at the end of the workday or when you will be gone for an extended period.
- ☐ Computer (laptops, tablets, phones, etc.) screens should be locked when the workspace is unoc-cupied.
- ☐ Portable computing devices such as laptops, tablets and mobile phones should be secured in locked storage when not attended or at the end of the workday.
- ☐ External storage devices such as CD's, DVD's, or USB drives should be secured in locked storage when not in use or not attended.
- ☐ File cabinets, drawers and storage lockers containing Confidential or Sensitive information should be kept closed and locked when not in use or not attended.
- ☐ Keys used for access to Confidential or Sensitive information should not be left at an unattended desk
- ☐ All printers and fax machines should be cleared of papers as soon as they are printed; this helps ensure that Confidential or Sensitive documents are not left behind for the wrong person to pick up.
- ☐ Upon disposal*, Confidential and/or Sensitive documents should be shredded or placed in locked confidential disposal bins.

**Ensure UTRGV record management and retention policies are followed when disposing of any UTRGV official records [HOP ADM-10-102]*

Data Privacy Day 2018

By StafSafeOnline.org Data Privacy Day 2018 MEDIA BACKGROUNDER

Led by the National Cyber Security Alliance (NCSA) in the United States, Data Privacy Day – held every year on January 28 – commemorates the 1981 signing of Convention 108, the first legally binding international treaty dealing with privacy and data protection. Launched in Europe and adopted in North America in 2008, Data Privacy Day brings together businesses and private citizens to share the best strategies for protecting consumers' private information.

The 2018 Data Privacy Day theme centers on "Respecting Privacy, Safeguarding Data and Enabling Trust." Following a year of massive data breaches at places like Equifax, Verizon, the NSA and Uber, it is necessary for people to learn how to better secure their personal information. And with 68 percent of consumers saying they don't trust brands to handle their personal information appropriately, Data Privacy Day also encourages businesses to be more transparent about how they collect and use data.

WHY WE SHOULD CARE ABOUT ONLINE PRIVACY

We produce a nearly endless stream of data in our daily lives. Seventy-seven percent of Americans now own smartphones, up from a mere 35 percent in 2011. Today we conduct much of our lives on the internet and on our connected devices, yet few people understand the enormous amount of personal information that is collected and shared from our devices and the services we use online. This data can be stored indefinitely, and our personal information can be used in both beneficial and unwelcome ways. Even seemingly innocuous information – such as your favorite restaurants or items you purchase online – can be used to make inferences about your socioeconomic status, preferences and more. The absence of strong online consumer protection laws in the U.S. means that many companies have the opportunity to monitor their users and customers' personal behavior and sell the data for profit. Consumers need to understand the true value of their information and how it is collected, used and shared in order to make informed decisions and better manage their personal data.

WHAT IS THE DIFFERENCE BETWEEN PRIVACY AND SECURITY?

Security refers to the ways we protect ourselves, our property and personal information. It is the first level of defense against unwanted intruders. Privacy is our ability to control access to our personal information. Although the U.S. Constitution does not explicitly define privacy, U.S. law has come to recognize that individuals have a right to privacy in many different contexts.

Top Tips to Securely Using Social Media

Social media sites, such as Snapchat, Facebook, Twitter, Instagram, and LinkedIn, are amazing resources, allowing you to meet, interact, and share with people around the world. However, with all this power comes risks--not just for you, but your family, friends, and employer. In this newsletter, we cover the key steps to making the most of social media securely and safely.

- Posting—Be careful and think before posting. Anything you post will most likely become public at some point, impacting your reputation and future, including where you can go to school or the jobs you can get. If you don't want your family or boss to see it, you probably shouldn't post it. Also, be aware of what others are posting about you. You may have to ask others to remove what they share about you.

- Privacy—Almost all social media sites have strong privacy options. Enable them when possible. For example, does the site really need to be able to track your location? In addition, privacy options can be confusing and change often. Make it a habit to check and confirm they are working as you expect them to.

- Passphrase—Secure your social media account with a long, unique passphrase. A passphrase is a password made up of multiple words, making it easy for you to type and remember, but hard for cyber attackers to guess.

- Lock Down Your Account— Even better, enable two-factor authentication on all of your accounts. This adds a one-time code with your password when you need to log in to your account. This is actually very simple and is one of the most powerful ways to secure your account.

- Scams—Just like in email, bad guys will attempt to trick or fool you using social media messages. For example, they may try to trick you out of your password or credit card. Be careful what you click on: if a friend sends you what appears to be an odd message or one that does not sound like them, it could be a cyber attacker pretending to be your friend.

- Terms of Services—Know the site's terms of service. Anything you post or upload might become the property of the site.

- Work—If you want to post anything about work, check with your supervisor first to make sure it is okay to publicly share.

Follow these tips to enjoy a much safer online experience. To learn more on how to use social media sites safely, or report unauthorized activity, check your social media site's security page.

Subscribe to OUCH! and receive a copy every month - www.sans.org/security-awareness/ouch-newsletter

Do **YOU** have an idea for a topic? Would you like to include something in particular to this newsletter? Any comments or suggestions are **ALWAYS** welcome!

Feel free to submit your thoughts by visiting our website:
bit.ly/utrgvisonewsletterfeedback


DON'T
GET
SMACked
Check your
Social Media
Access Controls
utrgv.edu/is/en-us/
resources/social-media


DATA
PRIVACY
DAY
JAN. 28
PERSONAL
INFORMATION
IS LIKE MONEY.
VALUE IT. PROTECT IT.
Respect Privacy, Safeguard Data and Enable Trust.
Get Involved
STAYSAFEONLINE.ORG/DATA-PRIVACY-DAY
PrivacyAware

If you need to report an incident

Visit our website (www.utrgv.edu/is) if you need to report a security incident. Some incidents may require you to report them to both the ISO and the UTRGV Police Department (PD) or to Information Technology (IT). For example any loss or theft of a University owned computer (e.g. workstation, laptop, smartphone, tablet) has to be reported to the ISO and the UTRGV PD. Similarly, ransomware infected UTRGV owned computers must be reported to the ISO and IT.

REPORT INCIDENT

The University of Texas Rio Grande Valley™

Information Security Office

Locations:

- Sugar Road Annex (ESRAX) Building
- R-167 Rusteberg Hall (BRUST) Building (*by appointment*)

Phone: (956)665-7823

Email: is@utrgv.edu

Visit us on the web and social media!
www.utrgv.edu/is
www.facebook.com/utrgviso
www.twitter.com/utrgviso

The mission of the Information Security Office is to provide support to the University in achieving its goals by ensuring the security, integrity, confidentiality, and availability of information resources. The role of the Chief Information Security Officer (CISO) is to maintain oversight and control of the enterprise information security program for the University.

Services We Provide

GOVERNANCE, RISK AND COMPLIANCE

ASSET AND VULNERABILITY MANAGEMENT

ENGINEERING AND INCIDENT RESPONSE

AWARENESS, COMMUNICATION AND OUTREACH

Give us YOUR FEEDBACK!
bit.ly/utrgvisonewsletterfeedback