We use this space to provide a 'curated' set of IT security notices (those most likely to affect us in our type of business). If you have IT-security questions please send those on to the Help Desk and we will do our best to answer.

Staying Safe from Tax Scams

March 2018 Volume 13, Issue 03

From the Desk of Thomas F. Duffy, Chair

Though Benjamin Franklin is often quoted as saying “in this world, nothing can be said to be certain, except death and taxes,” an updated version for the current day would need to include tax scams. As people nationwide seek to file their tax returns, cybercriminals attempt to take advantage of this with a variety of scams. Hundreds of thousands of U.S. citizens are targeted by tax scams each year, often only learning of the crime after having their legitimate returns rejected by the Internal Revenue Service (IRS) because scammers have already fraudulently filed taxes in their name. The IRS reported a 400% rise in phishing scams from the 2015 to the 2016 tax season. In the state, local, tribal, and territorial government sector during 2017, approximately 30% of all reported data breach incidents were related to the theft of W-2 information, which was likely used for tax fraud. Read on.

Good to know...

New Device for the Holidays? Check your CyberSecurity!

That new device you get or give during the holidays. Whether it's a smartphone, laptop, desktop, tablet, or another device, check out the below tips to help you protect your new technology and secure your personal data.

Why does cybersecurity extend beyond computers?

Actually, the issue is not that cybersecurity extends beyond computers; it is that computers extend beyond traditional laptops and desktops. Many electronic devices are computers—from cell phones...
Vulnerabilities in modern computers leak passwords and sensitive data.

Meltdown and Spectre exploit critical vulnerabilities in modern processors. These hardware vulnerabilities allow programs to steal data which is currently processed on the computer. While programs are typically not permitted to read data from other programs, a malicious program can exploit Meltdown and Spectre to get hold of secrets stored in the memory of other running programs. This might include your passwords stored in a password manager or browser, your personal photos, emails, instant messages and even business-critical documents.

So, What Are We Doing About This?

We need to update and patch all machines on the network. This is going to take some time, some of the patches are not even available yet. We also may have to replace some mission-critical computers to fix this. ITS will work alongside and with University technology partners as we mitigate the threat together.

In the meantime, we need you to be extra vigilant, with security top of mind and Think Before You Click.

Tax Time Guide: Protect Personal, Financial, Tax Information and Computers

The Internal Revenue Service (IRS) has released tax-time advice intended to help the public protect their personal and financial data and computers. Recommendations include using strong passwords, backing up files, and using robust security software to help block malware and viruses.

Users and administrators are encouraged to review this week’s IRS Tax-Time Guide and US-CERT Tip ST05-014, Real-World Warnings Keep You Safe Online, for additional information.

Please be aware of a new campaign of phishing emails that targets users filing taxes. These emails could attempt to steal your personal information. Remember to never open attachments you did not expect to receive. If you receive a link in an email like this, you can also hover over the link to see the real web address you will be sent to. Be sure to verify the site’s credibility before ever logging in.
The FBI has provided 4 great brochures with tips for keeping safe while using Social Networking, please read on.

The Federal Trade Commission (FTC) has released an alert on fraudulent mobile apps designed to exploit consumers. Some fake apps may steal personal information such as credit card numbers. By taking precautions, users can protect themselves and their private data.

US-CERT encourages users and administrators to refer to the FTC Scam Alert and background article on Understanding Mobile Apps.

When I rent a car, it's fun to get all the bells and whistles – like navigation, hands-free calls and texts, streaming music and even web browsing. But did you know that cars with these features might keep your personal information, long after you've returned your rental car? Here are some things to keep in mind when renting a connected car.

https://www.consumer.ftc.gov/blog/what-your-phone-telling-your-rental-car

Traveling Securely

Summer is finally here and for many of us that means it's time to get away! It's not surprising that many cyber criminals target travelers. Luckily, with a little care it's possible to protect yourself and avoid potential problems.