In this edition of our IT bulletin, we bring you a diverse range of articles that explore the intersection of technology and education, security, and sustainability. First, we delve into AI voice spoofing, an emerging threat that manipulates audio recordings. We highlight Raider PC Mart, a TTU online platform facilitating the exchange of used TTU computing equipment within our university that helps extend the lifespan of our technological investments. We provide information about another valuable service, our Computer Based Training (CBT) solution, Udemy, which offers thousands of hours of world-class content. With Summer in full swing, we share information on the importance of parental involvement in their child’s digital life, providing insights into different parental controls for safer online experiences. We also provide some summer travel tips for our summer vacationers to keep their data safe and secure. Lastly, we share information about Microsoft’s retirement of wikis in Teams, with a recommendation to quickly migrate your content to Microsoft OneNote to prevent data loss. As we continue to navigate the evolving landscape of technology, these articles offer valuable perspectives and guidance for the TTU community. Remember, stay informed, stay secure, and as always - Go Tech!

—Sam Segran, Vice President for IT and Chief Information Officer

Unmasking AI Voice Spoofing

In an ever-evolving technology landscape, the emergence of AI voice spoofing or voice cloning presents a novel challenge in the realm of digital trust. This technique, reminiscent of its email and text counterparts, pushes the boundaries of deception by manipulating audio recordings to mimic someone’s voice. This article delves into the implications of this evolving threat, its parallels to email and text spoofing, and the steps being taken to preserve trust in our interconnected world.

Understanding AI Voice Spoofing

AI voice spoofing represents an evolutionary leap in cyber deception, harnessing sophisticated algorithms and deep learning techniques to replicate an individual’s unique vocal traits. By utilizing a small voice sample, these algorithms generate remarkably realistic imitations, blurring the lines between genuine and synthetic voices. The concerns surrounding this technology extend to impersonation, audio evidence tampering, and voice-based phishing attacks. From precise syllable pronunciations to nuanced intonation patterns, this technology can create a near-identical vocal replica.

Combatting AI Voice Spoofing

As AI voice spoofing gains prominence, researchers, industry experts, and technology companies are actively developing robust countermeasures. Advanced voice biometrics systems are emerging to detect synthetic voices and distinguish between authentic and manipulated audio recordings. Employing state-of-the-art algorithms, these systems analyze various acoustic nuances, including pitch, timbre, and pronunciation patterns, to uncover anomalies indicative of AI-generated voices.

Simultaneously, real-time monitoring tools are under development, designed to identify AI voice spoofing attempts during live conversations or phone interactions. By harnessing machine learning and behavioral analysis, these systems capture subtle cues that betray voice manipulation, bolstering security during voice-based transactions.

Effectively mitigating the risks associated with AI voice spoofing necessitates a multi-faceted approach. Heightened user education regarding voice manipulation techniques and their inherent risks is pivotal. Individuals must exercise caution when divulging sensitive information over the phone or through voice-based platforms.

How to Avoid Voice Spoofing Scams

- **Stay Educated**: Familiarize yourself with voice manipulation techniques and the risks associated with AI voice spoofing.
- **Exercise Caution**: Avoid sharing sensitive information over the phone or through voice-based platforms, especially with unknown or unverified callers.
- **Verify Caller Identity**: Take steps to verify the identity of callers before divulging personal or confidential information.
- **Be Skeptical of Requests**: Maintain a healthy skepticism towards unexpected or unusual requests made over the phone, especially if they involve sensitive data or financial transactions; if in doubt, do not divulge your private information.
- **Keep Software Updated**: Ensure that applications, devices, and operating systems are up to date with the latest security patches.

As AI voice spoofing emerges as a new threat in the digital realm, preserving digital trust and securing your personal data demands an understanding of its implications. However, it’s important to recognize that AI voice spoofing is merely the next progression of traditional email and text spoofing tactics. The strategies that have proven effective in mitigating email and text spoofing can be applied to counter this emerging challenge as well. A healthy dose of skepticism should be maintained towards unexpected or unusual requests received over the phone just as with texts or email, especially those involving sensitive data or financial transactions. It is crucial to remember that reputable organizations typically do not solicit sensitive information without prior arrangement. When uncertainty arises, refrain from disclosing private information until the caller’s identity and intentions are verified. By remaining vigilant and well-informed, you can help to ensure the utmost security of your personal data in the face of this emerging challenge.
TTU IT Equipment Exchange with Raider PC Mart

Raider PC Mart allows departments to electronically connect with other departments that may be interested in outgoing computing equipment and peripherals before the equipment is transferred to Property Surplus. These technology exchanges extend institutional technology investments, making the use of computing equipment more efficient.

Raider PC Mart allows individuals authorized by the department head to post computer equipment no longer needed in their department. In addition, they can review equipment posted by other departments and express interest in available equipment. While inventory transfer paperwork and procedures are required prior to the exchange, Raider PC Mart is a voluntary utility designed to foster communication and extend the life of TTU’s IT equipment investment. The departments involved are responsible for the terms of the exchange. The system is designed only for the purposes of computing equipment exchange. We encourage you to dust off that unneeded computer or printer and list it on Raider PC Mart—recycle and extend institutional technology investments!

Computer Based Training (CBT): Anytime, Anywhere

The TTU IT Division offers learning and professional development “anytime, anywhere” for the TTU community with free online Computer Based Training (CBT), a service TTU contracts from Udemy. CBT is an online, self-paced, interactive training system with over 19,000 courses available to all TTU students, faculty, and staff. CBT offers courses for professional development, resume enhancement, just-in-time training, and on-the-job training.

Courses are taught by a diverse set of world-renowned instructors, leveraging technology to engage learners. Thousands of courses are also available in French, German, Japanese, Portuguese, and Spanish. CBT supports learners who want to advance in their current profession or gain a more profound understanding of topics of personal interest.

Features Include:

- **Unlimited access** to 19,000+ top courses selected from cbt.ttu.edu – anytime, on any device;
- **Fresh content** taught by global, credentialed instructors;
- **Courses for professional development**, including leadership, marketing, sales, software development, programming, and IT;
- **24/7 access** to on-demand learning on your desktop, laptop, tablet, or smartphone (available on both Android and iOS);
- **Download courses** or individual lessons for offline viewing;
- **In-depth courses** from 2 hours each to 40 hours, with individual lessons under 10 minutes; and
- **Shorter Smart Tips** courses (around 5 minutes)

As a Parent, How Do You Stay Involved in Your Child’s Digital Life?

Article reprinted from https://staysafeonline.org/, June 10, 2022

Mobile Devices

You can set parental controls on almost all mobile devices your child uses, including smartphones and tablets. Mobile phone service providers have different options for controlling privacy and usage, filtering content as well as location and monitoring settings.

Usage Controls

Today’s computer operating systems allow parents to turn off features, such as video/image downloading, text messaging and internet access. These controls can also be used to limit the number of calls or texts the device receives. You can also set time restrictions, usually for either the entire device, specific apps, or both.

Filter Content

With content filtering, you can block certain websites from your children to allow for safer web browsing. These content filters can be installed on either computers or mobile devices. Some filters can also limit video access and other multimedia.
Location Monitoring Systems
These controls allow parents to track their children’s whereabouts using GPS systems that are built into devices. These are especially useful on mobile devices like phones. Not only are they useful for seeing the location of your children, but they can also help you locate a lost or stolen device.

Additional Resources
- Entertainment Software Rating Board: Resources for Parents
- Family Online Safety Institute (FOSI): Good Digital Parenting
- FTC: OnGuardOnline.gov
- Google Family Safety Center
- Microsoft: Getting started with Microsoft Family Safety
- Microsoft: Family Safety

ISP Resources
- AT&T: Internet Safety Guide—Parental Controls
- Xfinity: Set Up Parental Controls for the Internet
- Cox: Parental Controls
- Mediacom: Parental Controls
- Verizon: The Smart Family

Summer Traveling Tips
Travelers may face an increased risk of identity theft if they carry debit/credit cards, passports, and other official forms of personal identification. As a result, vacationers are regularly targeted by criminals, who are just as likely to go after your personal information as they are your laptop or smartphone. To help protect your identity and information, the TTU IT Division recommends the following best practices while traveling:

- Carry a limited number of credit cards to limit your exposure to theft. We recommend that you notify those credit card companies about your travel and make sure you know how to contact them in the event your credit cards are stolen or lost;
- Take advantage of the hotel safe rather than leaving personal items in your hotel room;
- If you make travel arrangements using a mobile device, avoid storing transaction information, such as login information, credit card number, or billing address, on your mobile device. Remember that saved information could be stolen along with your phone;
- Protect your computers and mobile devices (including phones) with passwords;
- Public wireless connections are not secure, so avoid using them for secure transactions, such as transactions requiring a login; and
- Stay alert! It is easy to let your guard down while relaxing on vacation, but it’s essential to be aware of your surroundings and the people around you.

Retirement of Wikis in Microsoft Teams
Microsoft has announced that they have begun retiring the built-in Wiki application in Microsoft Teams. Teams that use this feature will notice a banner at the top of their Wiki containing instructions on how to migrate their content to Microsoft OneNote.

The TTU IT Division recommends migrating any Wiki content to Microsoft OneNote as quickly as possible to prevent data loss.

Key dates
- June 2023 – The Wiki tab in a channel will not be supported.
- January 2024 – The Wiki tab and Wiki app will no longer be accessible in Teams. However, Wiki files will still be downloadable from SharePoint.

For assistance with migrating your Teams Wiki content, or for any questions or additional information, please contact IT Help Central at (806) 742-4357 (HELP) or via email at ithelpcentral@ttu.edu.