VOLUME 2 | ISSUE 1

THE TECHNOLOGY BYTE

NEWSLETTERS FROM YOUR TECHNOLOGY GUIDE:
ACE TECHNOLOGY GROUP

OVERVIEW:

NEW YEAR PREDICTIONS

Emerging Trends in Cybersecurity

Current and emerging cybersecurity trends should be on the radar of individuals and businesses heading into 2022.

AI-powered cybersecurity is an emerging trend that many businesses are now using to counteract AI-powered cyberattacks. AI-powered security can detect patterns of behavior that send red flags when something is out of the ordinary.

Ransomware threats are a trend that is here to stay. Ransomware typically involves infecting devices by locking files until a ransom demand is satisfied. More recently, cybercriminals who have access to computers use USB devices and directly infect machines. These attacks target critical companies that could endanger lives, like hospitals or gas lines.

The attack on the Internet of Things (IoT) is predicted to reach 18 billion in 2022. Attacks on household appliances, like refrigerators or dishwashers, give a cybercriminal access to the phone or computer the data is stored.

Education is the key to avoiding becoming a victim. Always consult your IT company if you suspect suspicious activity.

ACE Technology Group

RECENT SECURITY BREACHES IN THE U.S.

Shutterfly
Exploit: Ransomware

Maryland Department of Health
Exploit: Hacking

Federal Bureau of Investigation (FBI)
Exploit: Account Takeover

UNDER THE HOOD

VoIP Benefits When Working From Home

As we embark on 2022, some companies and their employees continue to work remotely. Businesses with VoIP, Voice-Over-Internet Protocol can continue to answer calls as they would if they were in an office building. VoIP calls are routed over an internet connection, making calls secure with clear voice quality.

Staff working from home can use a physical phone or computer to make and receive calls. VoIP software mimics the office phone number so employees can keep their phone numbers private.

Most VoIP services offer email transcriptions when someone leaves a voicemail, a much-added benefit when multitasking.
An additional benefit to VoIP is it promotes workflow with fellow employees. Some employees may not be in the office, but using VoIP, users can still see if their co-workers are on a call or away from their phones.

Learn More About aceVoIP: https://bit.ly/aceVoIP

Home Office & Security for 2022

CHRIS'S CORNER

Expert Advice From The Owner

Working from home is officially here to stay for some companies and their employees. In 2021, a 36 percent increase of office managers worked outside of their offices after the pandemic. For employees and employers, there are plenty of benefits when working from home however, if network security implementations are low, then companies could be severely at risk.

As we head into 2022, experts predict cybercriminals will increase deepfake audio spear-phishing attacks. Cybercriminals use deepfake audio to imitate a fellow employee or an executive to convince someone to give them access to sensitive information or access to the company's network. Because people are working from home, they can't see if a fellow employee is at their desk or on the phone. They also cannot physically go over to the person to confirm any requests they may be receiving, and cybercriminals are using this to their advantage.

Sticking to official sites and marketplace app stores when downloading software and updates will avoid malware and scams. Carefully reading reviews will also help users catch any possible red flags. Most importantly, users should never click suspicious links sent from unknown senders. For example, clicking a link regarding purchases you did not make could lead to ransomware attacks, installing malware, or spyware on their device. Wherever possible, consumers and businesses should enable Two-Factor Authentication (2FA) or Multi-Factor Authorization (MFA). Enabling MFA protects 99.9% of users against social engineering, password attacks, and phishing scams.

The start of the New Year is a great time to set some home office safety and cybersecurity goals. Take time this month to update your passwords, enable MFA, and maintain an organized home office.

LATEST IN CYBER SECURITY

WFH CyberSecurity Tips

2020 and 2021 had more Americans working from home than ever before. As we head into 2022, remote work is here to stay. Follow these cybersecurity tips to keep your devices and data safe from cybercriminals when working from home.

A basic but IMPORTANT security tip is to follow your company's Work From Home policy and Cybersecurity guidelines. Companies and organizations have these policies to protect themselves, their employees, and sensitive data from cybercriminals. If you are unaware of your company's security measures, contact your IT department.

Another, but just as important tip, is to keep your personal and your work devices separate. By keeping them separate, you can avoid accidentally downloading malware, spyware, or compromising your company's data. Having two devices not only keeps your company's data safe, but it's also the easiest way to set boundaries between the two areas of your life.

In addition, a secure WiFi network is just as crucial at home as it is in the office. A hacker could breach your home WiFi and access your company's data or even use your WiFi network for criminal behavior. The best way to secure your WiFi router is to create a unique password. Never work using public WiFi as they are most susceptible to cybercriminal attacks. The safest and most secure place is your home's protected WiFi.

One of the most effective ways to keep your identity secure is to enable a Two-Factor-Authentication (2FA) or Multi-Factor-Authorization (MFA) whenever possible. Enabling an MFA requires additional "proof" that the correct person is accessing the account and not a hacker. If you receive a suspicious email request or believe there is unusual activity, contact your company's IT department immediately.

By following cybersecurity tips and best practices, companies and individuals can avoid risks and costly mistakes at home and at the office.

REMOTE WORK GUIDE

DO'S AND DON'TS

Working remotely has many benefits but also creates many cyber security risks. Use this handy list of Do's and Don'ts to help you protect your company and sensitive material.

DO	DON'T
Read & acknowledge your companies Remote Work & Bring Your Own Device (BYOD) policies & procedures.	Ignore the guidelines in your company's policies. Make the required changes if any.
Avoid using your personal device for work and restrict the use of company-issues devices for personal use.	Let family or friends use your company-owned devices.
Protect the data you are accessing by using a Virtual Private Network (VPN) to log into the company network	Use public WiFi to access the company network without using a Virtual Private Network (VPN)
Use strong unique passwords on all your devices and accounts to prevent unauthorized access	Use your default WiFi router password
Ensure all personal devices are secure with anti-virus and anti-malware software	Forget to update your router's firmware & ensure the software on all devices on your home network is up to date
Be extremely cautious of email phishing scams	Send electronic payments without following your company's policy for verifying payment requests

CYBESECURITY TERMS TO KNOW

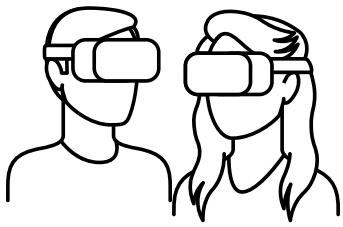
Deepfake: *noun*

a fake, digitally manipulated video or audio file produced by using deep learning, an advanced type of machine learning, and typically featuring a person's likeness and voice in a situation that did not actually occur. *(Dictionary.com)*

REMINDER

PLEASE LEAVE YOUR PC OR LAPTOP ON OVERNIGHT AND ON THE WEEKENDS SO WE CAN REMOTELY RUN NECESSARY UPDATES

Augmented Reality to Improve Online Shopping Experiences



The future of Augmented Reality (AR) will make online shopping experiences easier by allowing shoppers to interact with a virtual representation of the product before purchasing.

From the comfort of their home, online shoppers will be able to get a personalized view of products by virtually examining them without ever leaving the comfort of their homes. Shoppers will have the ability to customize certain features such as size, color, or designs. Product models will be created in 3D, making online shopping as close to reality as possible.

There are many benefits to AR online shopping. For example, IKEA features an AR app for online shoppers to virtually place and view pieces of furniture in their space to ensure the product is a fit. Another big benefit, shoppers will save time. No traffic and no struggle to find the perfect parking spot! Interactive mirrors will allow shoppers to try on clothes, put outfits together, therefore, reducing the number of returns shoppers need to make.

Over the next several years, Augmented Reality will play a big role in online shopping experiences. eCommerce sites will learn more about technology and their customer's online shopping strategies creating a unique virtual shopping experience.

EMPLOYEE SPOTLIGHT: CHRIS

Get to know your friendly ACE team!

Gained engineering experience with the US Navy, Bell Atlantic Business Systems Services and Penn State College of Engineering. After graduating from Penn State with a BS in Computer Engineering, Chris went on to be a Software Engineer for Lockheed Martin, DecisionOne, Medical Broadcasting Company, and Aventis Behring before finally striking out on his own.

Chris served as the Chief Technologist for a large medical practice of over 100 practitioners. He engineered, built, and maintained their electronic medical records and enterprise infrastructure platforms that spanned over 40 locations, 50 servers, 700 PCs, and two redundant data centers. Chris also is the primary engineer for all the technology that ACE uses to provide managed services to our customers.

Known for troubleshooting and problem-solving, Chris quickly identifies and resolves issues. With the knowledge that comes from over 20 years' worth of experience, the Navy's Troubleshooting Honor Award, and Lockheed Martin's Pride Award, clients confidently can and do say, "he's good at what he does."

POWER COMMANDS

Only screenshot the part of the screen you want

For Windows: Go to "Start" and then "Snipping Tool". Then you drag the area you want.

For Mac: Command + Shift + 4 brings up the tool.

Bring back a closed tab

For Windows: Press Ctrl + Shift + T to reopen the most recently closed tab.

For Mac: Press Command + Shift + T.