VOLUME 2 | ISSUE 6

THE TECHNOLOGY BYTE

NEWSLETTER FROM YOUR TECHNOLOGY GUIDE:
ACE TECHNOLOGY GROUP

OVERVIEW:

GOODWILL RANSOMWARE DEMANDS PUBLIC ACTS OF CHARITY AS PAYMENT

Move over Robinhood! GoodWill ransomware attack forces victims to record acts of kindness to recover stolen files.

Traditionally cybercriminals steal files or data and demand cryptocurrency as payment. A cyber "Robinhood", if you will, is demanding victims to record acts of charity and post on social media in exchange for their files. While this ransomware appears as a stand for social justice, some people see it as public humiliation for the victim.

The ransom demand has three key activities that the victim must follow in order to get their data back.

- **GoodWill Activity 1:** Provide clothes and blankets to the homeless, record the act, and post on social media with a specific frame the hacker provides, and then email a screenshot to the hacker.
- **GoodWill Activity 2**: Take 5 poor children (under age 13) from your neighborhood and treat them to the food they love to eat. Treat them like family. Record it, post it, and email a screenshot to the hacker.
- **GoodWill Activity 3**: Visit a local hospital and pay the medical treatment bill for someone in need. Record audio of the conversation, post it, and email details to the hacker.

While we can all agree these activities are harmless and are helping those in need, we can also agree that stealing and forcing someone to do something against their will is still a crime.

RECENT SECURITY BREACHES IN THE U.S.

The U.S. Drug Enforcement Agency (DEA)
Exploit: Hacking

Omnicell - Healthcare Tech
Exploit: Ransomware

AGCO: Agricultural Machinery Manufacturer
Exploit: Ransomware

WHAT IS VISHING?

Vishing is shortened version of the phrase 'voice phishing', vishing is when the attacker obtains the victim's data over the phone by getting them to reveal identifying information. Vishing is not exclusive to any one type of phone call and can occur over a landline, mobile line, or VoIP (voice over internet protocol).

It's difficult to verify a caller when you can't see them – you usually ask questions and trust what they say. But with cybercrime in today's world, you should never assume that the caller is safe.

Tips to protect yourself from vishing scams:

- Ask where they are calling from and for a callback number.
- Never give out any identifying information or confirm what they might ask you.
- Do not answer unknown or suspicious calls.
- Never give out Personally-identifying information (PII)

Read More

Be Alert for Interview and Job Scams

CHRIS'S CORNER

Monthly Expert Advice From The Owner

Likely, your employees will not be forthcoming that they are, or might be, looking for a new or additional job in the future. We wanted to bring awareness to interview scams because whether an employee is looking for a new job or not, they likely know someone who is.

There can be one or multiple red flags that can indicate a fraudulent job post.

- Direct contact from an interviewer for a position or company you never applied to.
- The company has no online presence, including a website, LinkedIn, social media, etc.
- It seems too good to be true - trust your gut - if they're offering an unrealistic salary for the role it's an indicator of a scam.
- Unprofessional correspondence - watch for grammar errors, typos, misspelled words, et
- Interviews conducted via chat - while video interviews have become the new norm chat interviews are a sure indicator that the job offer is a scam.
- A request to disclose personal information such as social security number, birth date, address, etc
- If you need to pay for the job interview - there's only one reason - SCAM

Cybercriminals are relentless. Encourage everyone to be aware of social scams including those related to job interviews. Remind those around you to never give out personal information to anyone they do not know.

LATEST IN CYBER SECURITY

Are Your Social Media Habits Safe?

There are lots of positive about social media including connecting with family and friends, but there are also plenty of hazards. There's no time like the present to reevaluate your social media habits.

When's the last time you reviewed your privacy settings? Today is the day if you've never checked your privacy settings on your social media accounts. In order to make your account easy to find and engage with, standard privacy safeguards are less secure. Check your privacy settings regularly, especially after a social media update, as privacy policies and settings change over time.

Data privacy settings can only protect you to a point. Think of social media like text messages: Once you send it to someone there is nothing to stop them from sending it to others. Remember when you share something with someone, what happens next with that information is no longer in your control. Once you hit send there are no privacy restrictions on text messages and screenshots of private messages can easily be shared on social media.

Deleting posts doesn't necessarily mean gone. And we all know that Snapchat's "self-destructing" messages don't actually disappear, can be screen-captured by the person on the receiving end and posted on social media.

Are you in the habit of asking questions? Cybercriminals and scammers love social media. Social media accounts are a treasure chest of personal information and it's easy for individuals to impersonate your friends and family. Before you click on a link, download a file, or accept a connection think about the possibility of malicious intent.

Five questions to ask yourself:

- Do I personally know this person?
- Am I already connected to this person?
- Does this seem legit?
- Do I know for sure this link/file is safe?
- Am I teaching my kids to police themselves?

Because our human tendency is to be trusting and open, it's important we all learn how to balance social sharing and safe sharing. Online safety can feel like a moving target, but these social media tips, which offer relatively basic precautions, can drastically improve the security of your personal information.

LEARN THE ROOTS OF GOOD SOCIAL MEDIA PRACTICES

DO

Be cautious if your friend sprouts unusual posts. Odd emails or posts could be from a hacked account

DON'T

Spread the same password over multiple social networking accounts

DON'T

Download or install software from social networking sites - keep it homegrown

DO

Weed out all the fake friends Don't accept connections from people you don't know

DO

Assume all posts are public and gets lots of sunlight. Think before you post.

Hackers and scammers use social media networks to try and harm you. limit the amount of information you share and the number of people you share it with.

CYBERSECURITY TERMS TO KNOW

TWO-FACTOR AUTHENTICATION (2FA) OR MULTIFACTOR AUTHENTICATION (MFA)

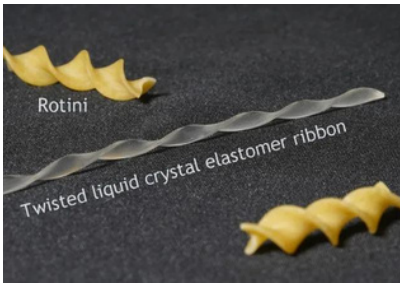
Also known as 2FA or MFA, this process requires one or more additional verification factors, which decreases the chances of a cyber attack.

REMINDER

AS A RESULT OF THE CHIP/HARDWARE SHORTAGE, IT'S HIGHLY PREDICTABLE THERE WILL BE DELAYS IN THE ARRIVAL OF ANY PRODUCTS YOUR COMPANY HAS ORDERED. WE WILL KEEP YOU UPDATED ON ANY ORDER STATUS.

NEW IN TECHNOLOGY

Move Over Macaroni - New Noodle Like Robot



Credit: Yao Zhao, NC State University

University of Pennsylvania (U Penn) and North Carolina State University researchers have teamed up to develop soft robots that demonstrate a concept of "physical intelligence". These soft robots have a structural design and use smart materials to navigate various situations without help from humans or computer software.

The Ribbon Robots are made of "liquid crystal elastomers" and shaped like twisted ribbon, making them look like clear pieces of pasta rotini. When a portion of the ribbon bot is touching a surface of 131 degrees Fahrenheit (Hotter than ambient air), it induces rolling motions. The warmer the surface, the faster it rolls.

The ribbon bots require no human or computer intervention to navigate. If one end of the robot touches an object, it slightly rotates to get around it. But if the center of the robot touches an object it "snaps" and releases stored deformation energy that causes the ribbon bot to "jump" slightly and readjust itself. The ribbon robot may need to snap a few times until it finds a clear path to move forward. The ribbon bot is similar to Robo vacuum cleaners, where it bounces off surfaces to navigate, but the ribbon bot requires no computer programming.

Researchers have used the ribbon robots in a variety of mazes and have shown they work well in desert environments, where they can roll, climb, and descend slopes of loose sand. The research shows how robots can be designed and capable of harvesting heat energy from natural environments. Read more

Watch the "Ribbon Bot" in action:
https://www.youtube.com/watch?time_continue=44&v=7q1f_JO5i60&feature=emb_logo

Get to know your friendly ACE team!

EMPLOYEE SPOTLIGHT: ERIC

Support Desk Technician; Philadelphia, PA;
Associates in Electronics Engineering

Eric has always been passionate about helping people and solving problems. For over 14 years, he's been working as a Support Desk Technician, with four of those years in a disaster recovery role. He has a knack for talking to customers and making them comfortable. Eric can explain technical issues and solutions to "non-technical" people easily. No geek speak here!

During the warmer months, Eric enjoys spending his free time at one of the local golf courses. During the colder months, be enjoys a good movie or gaming. Eric's favorite non-profit is the United Way. After being involved with clothing and school supply drives, he was able to see the positive impact it made on the community.

- One thing he will not give up is his sense of humor.
- Spends his weekends doing various outdoor activities or watching football.
- Wants to be remembered as someone who had an overall sense of warmth.

Meet the Rest of the ACE Team

POWER COMMANDS

Open new tab or window

For Windows: Ctrl + N

For Mac: Command + T

Hide all windows to the current app

For Windows: Win + D

For Mac: Command + H

Find us on LinkedIn