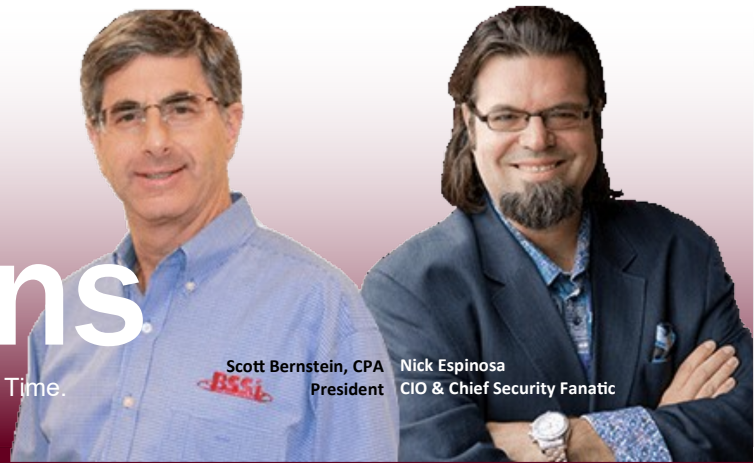
BSSi2 Innovations

Review Twice, Implement Once. Doing IT Right the First Time.



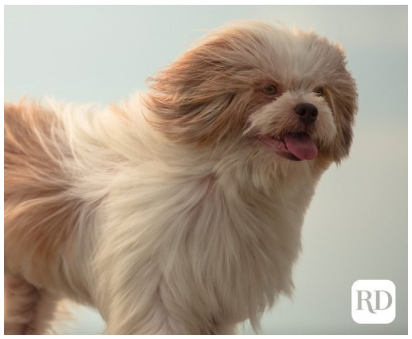
Scott Bernstein, CPA
President

Nick Espinosa
CIO & Chief Security Fanatic

The Lighter Side….

When you turn on the AC in the car and it blows hot air.

When you finally walk into the AC



When it's the end of summer and you give up on lookin good

Internet Safety Tips for Parents

In today's climate, is there anything more prevalent than the Internet? In fact, we've grown so accustomed to using it that the Internet now seems to help us meet any need or want. Unfortunately, we don't often think about the effect that has on our kids, who have never known a world without this level of technology.

For the most part, the Internet is an incredible boon to our children. They can look up anything they're curious about and will be met with more information than previously fathomed. Many of us remember visiting the library to research topics, and even then, resources were limited compared to what can easily be found online today.

While the Internet offers many benefits for kids, there are risks. That's why it's important to keep your children protected. Before your kids get a social media account or dive headfirst into the web, take the following security measures.

Parental Restrictions

Nearly every device that can connect to the Internet has some level of parental control. With computers and laptops, you can restrict what websites and apps your children visit. You can also specify which websites you want totally blocked. This is an option on many tablets and smartphones as well. With those, you can actually set time constraints and limits that make it so your child can only use the device for a certain amount

Continue on the next page...

Continued from previous page...
of time, and you can even completely restrict usage at night.

Potential Risks
When your children first start using the Internet, you must ensure they understand any potential risks. We all know people aren't always who they say they are on the Internet. Similarly, not all information found online is true. When your kids visit websites or use apps, remind them not to share any personal information about themselves. They should never give out their address, school information, phone number or even their e-mail address to anyone online. Even if the person requesting this information claims to be someone they know, they might not be. If your child is using social media, inform them not to accept friend requests from people they don't know. It's important that kids understand all of the risks to ensure they stay safe in the digital and physical world.

Get Familiar
If your children are using the Internet, you should become familiar with the websites and applications they use. Make sure all websites have the little padlock icon by them, which indicates they are safe websites. Look through the apps and websites your children frequent to ensure they're safe for them to use and do not contain any inappropriate content.

Lead By Example
Your children's first interactions with the Internet will most likely stem from you, so do your best to set a great example for them. This is your opportunity to model positive online habits for your children. Your social media posts should also be appropriate and not break any of the online rules you set for your own child. In their eyes, it won't be fair if you or someone else in the family can do things they cannot.

Our children are some of the most important people in our lives, so it makes sense that we would do everything in our power to keep them protected. Just make sure your protective efforts extend from the physical world into the digital world as well.

Business Tidbit

4 Ways to Better Protect Your Personal Information

Most people keep their personal information as secure as possible. They don't post their passwords on social media or share Social Security numbers with untrustworthy sources. These practices seem obvious, but there are smaller things we can do to provide better protection. You'll find four of those tactics here.

Dangers Of Unsecured WiFi – Hackers can use this connection to download malware on your devices.

Password Manager – You shouldn't use the same password between multiple accounts. Utilizing a password manager will help you keep track of different passwords.

Breached Companies – When a company's security is compromised, all of its customers' personal information can be exposed. Avoid working with these companies until they've offered improved security.

Think Before Posting – Be careful about what you share on social media. Revealing too much personal information can leave you vulnerable to a cyber-attack.

New Phishing Attacks Shame, Scare Victims Into Surrendering Twitter, Discord Credentials

A new wave of social media phishing attacks are now using scare tactics to lure victims into sending their logins.

First, a Twitter phishing attack was reported earlier last week. Threat actors would send direct messages to the victims, flagging the account for use of hate speech. They would then be redirected to a fake Twitter Help Center to input their login credentials.

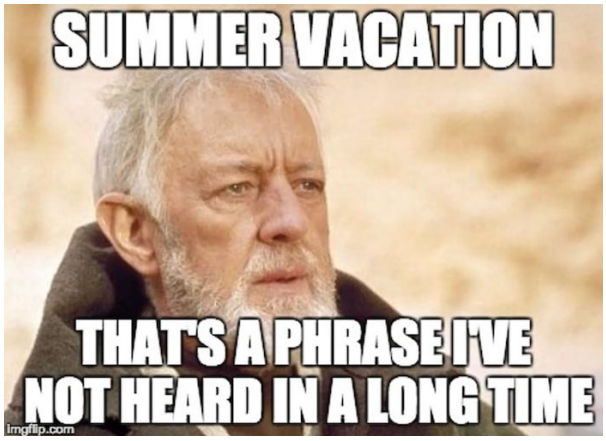
Then, a Discord phishing campaign was discovered by sending user a message from friends and/or strangers accusing the user of sending explicit photos on a server. The message also included a link, and if clicked would then lead to a QR code. This resulted in the account being taken over by the cybercriminals.

Social media have always been used for successful phishing attacks, using social engineering to manipulate victims to disclose confidential logins. And if successful, social media attacks can open the flood gates to the company network.

James McQuiggan, Security Awareness Advocate at KnowBe4, explained to Dark Reading about how effective social media phishing attacks can be, "A lot of the time, phishing attacks rely on the victim reacting to the email in an emotional state," he says. "The victim sees the email and responds without adequately checking the sender or the link."

These types of attacks are not going away anytime soon. And with the continual remote workforce, there is a higher risk of being targeted through your social networks without the word-of-mouth alerts you would get at the office from other employees. Get ahead of the curve now with your employees by implementing new-school security awareness training.

Stu Sjouwerman, CEO and Founder, KnowBe4, Inc.



The Lighter Side….

- Passwords are like underwear. You shouldn't leave them out where people can see them. You should change them regularly. And you shouldn't loan them out to strangers.
- Two antennas met on a roof, fell in love and got married. The ceremony wasn't much, but the reception was excellent.
- I told my wife she was drawing her eyebrows too high. She looked surprised.

August 2022

35 Aztec Court
South Barrington, IL 60010
(312) 752-4679
www.bssi2.com

"We make all of your computer problems go away without the cost of a full-time I.T. staff"

Shiny New Gadget of the Month

Oura Ring Generation 3

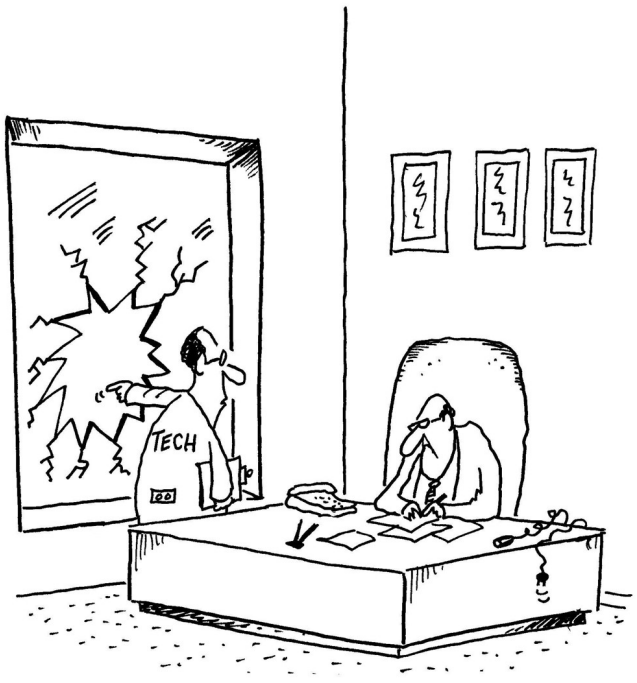
For the past few years, fitness trackers have become all the rage. Between Fitbits and the Apple Watch, nearly everyone has or is familiar with fitness trackers. One of the most common complaints about many fitness trackers is comfort. Oura decided to take the wristband out of the equation with the Oura Ring. The Oura Ring is a fitness tracker that you wear on your finger. It tracks sleep, activity and readiness measurements. This device is even more accurate than other fitness trackers since the finger is a better spot to record heart-rate data. Through temperature sensors, a library of informational resources and much more, the Oura Ring is the perfect fitness tracker for just about anyone who is looking to improve or maintain their physical health.

Stay up-to-date

Follow BSSi2 at:

www.facebook.com/bssi2

twitter.com/BSSi2llc



"Is that computer, down there, the one you were having problems with?"

CartoonStock.com