ISSUE
09
NOV
2014

new river computing

In this issue

IT SERVICES FOR BUSINESS

New River Computing is a locally owned IT services company dedicated to serving businesses in the New River Valley. The IT services we provide can help your business to increase revenue, decrease costs, and minimize risk.

The success of your business is important to the economic growth of our area. We take pride in providing the right computing infrastructure, services, and tools you need to succeed. Our close proximity allows us to respond quickly to service calls, and our expert staff takes pride in their relationship with you and your company.

1750 Kraft Drive
Suite 1000
Blacksburg, VA 24060

newrivercomputing.com

NRC at Chamber of Commerce Business Expo

Thank you to everyone who came out to the Business Expo and helped make it a success!

Hansen judges GNI pumpkin carving contest

Long-time NRC client, Gay and Neel, invited Hansen to be a judge at their annual Halloween pumpkin carving contest. It was a tough job with so many great entries in this year's contest!

NRC BIRTHDAYS

Chris - Nov. 6

10-YEAR ANNIVERSARY

11/08/2004 - 11/08/2014

New River Computing is celebrating 10 years of serving the New River Valley and surrounding areas!

George films first published 360-degree great white shark video

NRC's web designer, George Probst, was asked by Kolor, a France based technology company, to test out a 360-degree video rig on his last shark dive. As far as we know, this is the first footage of great white sharks to be published using 360-degree video technology. George tried out the Kolor Abyss 360 and managed to capture some close-up footage.

With the increasing popularity of head-mounted displays, such as the Oculus Rift, 360-degree video can create an immersive experience for viewers that will put them right in the middle of the action, and they won't even have to put on a wetsuit.

You can read more about the technology and view video samples shot by George at the Kolor website.

A male great white shark curiously approaches the Kolor Abyss 360. Photo courtesy of Barry Moorhead.

Matt goes head-to-head with phony Microsoft support scammer

Recently, scammers have begun claiming that they need immediate remote access to computers in order to fix security threats. Once they convince the user to allow them remote access in order to "take care of the problem," these savvy scammers then suggest installing fake malicious software—in order to "protect" the machine from future infections.

Just a few days ago, this happened to one of our clients. After receiving a phone call from someone claiming to be from "Microsoft Security Services," Sally, as we'll call her, was told that her computer had been hacked by someone in Austin, TX, and the "representative" claimed he needed to remote in to fix it right away.

Of course, Sally was panicked—a normal and reasonable reaction. Following the scammer's instructions, she went to a website, entered a few different numbers, clicked a few "ok" prompts, and then allowed the scammer to take control of her computer. As he worked through these steps with her, he used a few tricks to fool her into thinking that her computer was badly infected when, in fact, it was fine.

In order to trick Sally, the scammer pulled up legitimate, normal IT troubleshooting tools–such as Netstat, CPU Monitor, and Event Viewer to confuse her. For someone in the IT business, these screens are commonplace and useful for regular computer maintenance; for others, these look like a bunch of numbers and error messages which make no sense and cause serious alarm or fear that the computer is terribly at risk.

After driving this fear home, the scammer told Sally he could fix the problem for a fee. Sally then gave him her credit card number, but after a few minutes, the scammer claimed that the credit card transaction had failed and that he would need to try a different card. At that point, Sally said she wanted to call us, her IT support. Of course, the scammer tried to convince her otherwise, but she knew better.

After she told Matt what happened, he not only recommended she immediately cancel her credit card, but he immediately inspected her machine. After a few minutes on her computer, he realized something wasn't right. While performing various diagnostics, the mouse cursor moved, windows closed, and different things stopped running. Thinking it was Sally, Matt asked her to wait until he finished checking things out. But it wasn't Sally. Instead, it was the scammer still connected to the machine, and he was trying to install malware!

Immediately it was a race to win full control of the computer. The scammer closed programs and tools as fast as Matt could get them open. He eventually tried to lock the machine by installing a fake AV program with a bogus warning, "FBI Has Locked This Computer Due To Fraudulent Activity." He also tried to encrypt files in order to hold Sally's data for ransom. Luckily Matt was able to run a quick series of commands to end the rogue processes, before blocking the scammer's network access. He could have won; it was close—too close.

You might be wondering, "Isn't antivirus software supposed to protect my computer from this kind of stuff?" AV software does not, and more importantly, CANNOT protect a computer from every threat out there. It can go a long way to prevent your machine from becoming infected, but if you click "yes" enough times and give scammers access to your machine, even the best antivirus software will be defeated.

The biggest lesson to learn: educate yourself. User education is the most important factor to not getting infected and/or scammed. Be cautious before clicking "yes" and NEVER trust someone that calls out-of-the-blue, claiming he or she is from Microsoft or some other well-known software or security company. Microsoft and other such companies will NEVER call you to let you know that your computer is infected and then ask for money to fix it.