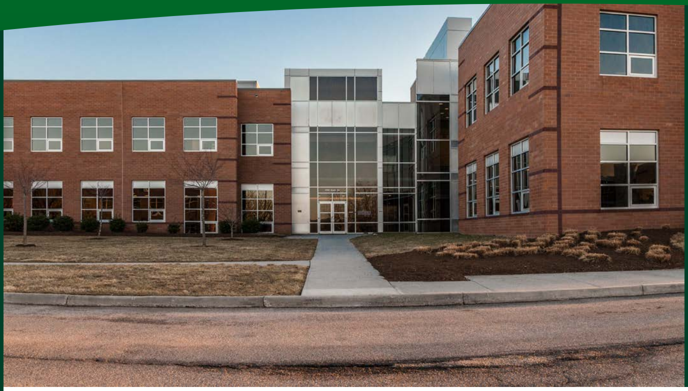
ISSUE
05
July
2015

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 fundraiser to benefit WRC or the NRV

New River Computing will be hosting a fundraising event to raise money for the Women's Resource Center of the New River Valley.

On August 18th at 4:30pm, Jeff and Matt are going to have their their luscious locks cut off in exchange for donations to the WRC!

The event will take place at the patio area of the Wikiteria Café at the Virginia Tech Corporate Research Center. (The Wikiteria Café is located just across the parking lot from the NRC offices.)

You can learn more about the event and donate to the cause at the fundraiser page on our website

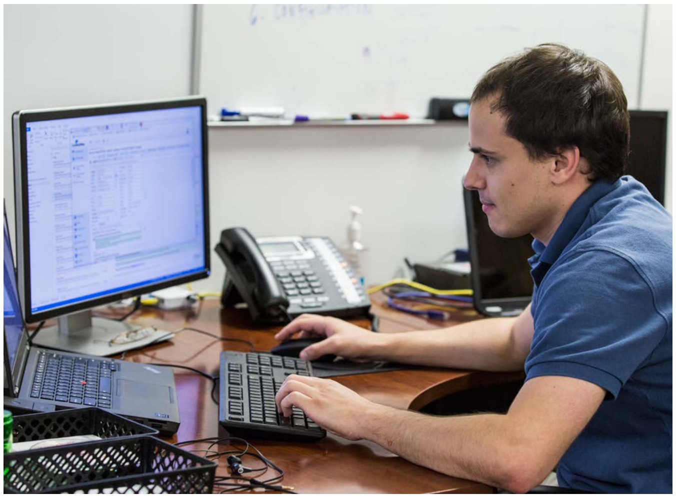
Bidding farewell to Tim Coyle

NRC would like to extend best wishes to Tim Coyle as he takes on his new position with the Montgomery County IT department.

As of June 26th, 2015, Tim exited full-time employment at New River Computing to begin his new role with the county. Tim started with us April, 2014, fresh from New River Community College. He has been a valuable asset around the office, helping wherever needed to provide personable support to NRC clients.

Please join us in wishing Tim the best in his future endeavors.

MEET ALEX ZAMMIT - NRC NEWEST TEAM MEMBER


Welcome Alex to the NRC team!

In college, Alex bounced around several fields of study trying to find what felt right. He graduated from Virginia Tech in 2012 with a Bachelor's degree in Consumer Studies. It was soon after that he realized he could take his passion for IT and pursue a career. Having always been the "computer guy" for friends and family, it seemed like a natural fit.

Immediately upon graduation, Alex returned to his hometown of Wytheville. Soon after, he joined Hodges, Jones & Mabry, P.C. to work as their in-house IT Specialist. While there, he managed the system and network administration for the business and provided technical support for employees.

Alex joined New River Computing in July of 2015 with 3 years of work experience under his belt. He is excited for the opportunity to assist a larger number of clients while continuing to grow within the IT field. Returning to Blacksburg was a big bonus to Alex as he really enjoys the area. The close proximity to the Appalachian Trail makes great access for hiking or backpacking during free time.

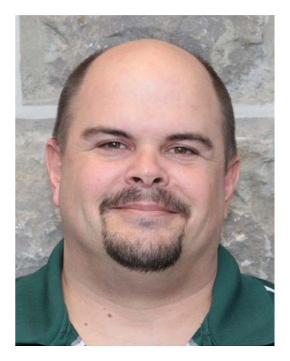
JULY BIRTHDAYS

July is a big month for birthdays here at New River Computing. We'd like to wish a happy birthday to Shana, Matt, Jeff, and Mark!

Shana Williams
July 13

Matt Stuart
July 15

Jeff Wynn
July 19


Mark Phillips
July 21

HIPAA security – keeping data secure

If you are a “covered entity” under the HIPAA Security rule, then you already know that your company (and thus your employees) collect a lot of protected health information (aka PHI). PHI is basically information about another person that is not for public knowledge but needed in order to conduct business. What business? Information that insurance companies need to process claims and health care professionals need for continuity of care.

Due to more recent mandates, healthcare entities have been required to use electronic health records where patient information is entered, accessed, stored, and distributed through computer and web based programs. The HIPAA security rule simply states that all data that pertains to PHI must be secure and not accessible by persons that do not need to know or by persons that intend to harm.

When we think of breeches in data we first think of “hackers.” According to Symantec, the healthcare industry is a hot target for hackers because medical records contain valuable personal information such as social security numbers, birth and death dates, billing information, etc. Criminals use this information to buy medical equipment, drugs that can be resold, or combine a patient number with a false provider number and file made-up claims with insurers.

Background systems managed by good IT Management firms (like NRC) can reduce the hacker threat. Now your agency is left to face the bigger threat of human error. According to USA today, 80% of the breeches that occur are rooted in employee negligence, by human error or the less frequent rogue employee. According to hipaajournal – 31% of the breeches reported are due to lost or stolen devices, 29% to criminal attacks, 8% to a malicious insider, and 29% to employee errors.

There are some simple steps each employee can take to minimize errors:

1. Stolen or lost devices (including removable media) should be reported to the Security Officer immediately.
2. Protect your passwords – don’t write them down, post them, or share them.
   Tip: develop a password based on a phrase, song, or poem that you know well!
3. Log off computer when not in use – if even for a minute.
4. Have a guest visiting your office? Close up your machine (ctrl + l should do it).
5. Don’t let others use your computer.
6. Don’t download programs on your computer without talking with IT (some of those programs look fine but are actually designed to glean information).
7. Be careful to whom you send that email! If you have to send email, encrypt it.

Administrator tips:

1. Limit BYODs unless there is a solid system for protecting information such as Windows 8.1 Enterprise solutions and Office 365.
2. Don’t let guests on your network! Set up a guest account!
3. Track activity! Watch out for rogue employees.
4. Immediately disable access to systems when employees leave the agency.
5. Have a solid policy in place that addresses how company equipment, software, and access is used.