NETWORKING 101

WEST VIRGINIA NETWORK (WVNET)

VOLUME 3, ISSUE 3

MARCH 2013

In this issue:

SOCIAL ENGINEERING ATTACKS AND YOU

A few weeks ago I received a rather odd email. It appeared to be from a coworker. The subject line read "Button" and the body of the text simply said "Tennis racquet, " followed by a URL with the word "strange". I wasn't really paying attention and for just a second I almost clicked the link out of habit, such as when you get emails from friends giving you something humorous to look at. Then I paused.

Ok, that's weird. First, this coworker likes golf. I never knew him to be into tennis. Second, he seemed to have sent the email to himself, me, several other coworkers, and some names I did not recognize. It was an odd list. Looking closer, I saw that the URL pointed to a website in Poland (futluz.pl). In the end, I did what I would normally do in such situations. I forwarded the email to my coworker and asked if he'd really sent it. Of course, he had not. This was a classic social engineering attack.

Social engineering attacks involve the art of manipulating people, often through their social connections to others, into performing actions or divulging confidential information. In this case, the intention was to trick users into visiting an infected website. How? Spoof an email making it look as if it's from person A sent to persons B, C, and D, where they know each other, and odds are you can get them to click on a hyperlink out of a sense of "Oh, I know person A." Of course, that link could be almost any kind of "drive-by attack", where getting a user to simply visit a booby-trapped website may be enough to infect their computer with malware. Due to the various security issues regularly found in software such as Oracle Java or Adobe Flash--common on most personal computers--and the fact that most users do not keep their systems fully updated, there is a window of opportunity during which users' computers are vulnerable. So trick a user into visiting such a website, and chances are good you can compromise their computer.

What made this one unique was that it happened to specifically target us here at WVNET. It appeared to come from a WVNET employee sent to several other WVNET employees. That's a first from my experience. Typically these are more random in nature. They usually involve an automated attack, where a virus that harvests a user's *(Continued from Above)* address book--for example, that of a friend whose computer got infected--then constructs emails as if from the infected user to people they know (again, exploiting their social connection to each other). Done in general, these are known as phishing attacks. Now if done by a human being with the intent to target folks at WVNET, this kind of attack would be called a spearphishing attack, as the intent is to target very specific people or organizations. There are other terms as well, such as whaling (targeting senior executives), but the point is still the same: exploit people's inherent trust in their friends and coworkers to get them to do something such as click a link that they might not otherwise do.

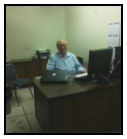
So please be aware of this. Most folks today know not to open emails from strangers, much as children generations ago were told never to take candy from strangers. However, now you must even be wary of emails that appear to be from people you know. This is more challenging, though often these emails give themselves away. Much like the infamous Nigerian 419 email scams where you receive emails written in poor English claiming you can get millions of dollars if you simply provide some basic information such as your name, bank account number, etc., your gut often detects something in the writing that doesn't fit. Unfortunately, these attacks are becoming more sophisticated, so simply "trusting your gut" may not be enough.

Continued on next page

The fundamentals of protecting yourself, however, have not changed. Do not rely on others to protect you. Only you have your best interests at heart. Keep your operating system and software patched with all the latest updates, paying attention to anything which interacts with the Internet, such as web browsers, browser plugins such as Flash and Java, email clients, instant messaging applications, etc. When web browsing, avoid unsavory websites, though if you have watched the news in recent months, even well-known and trusted sites like nbc.com have been guilty of infecting users with malware when their site was compromised for about 24 hours recently. And if you can handle the additional complexity, consider such things as addons for your browser which automatically disable all plugins and JavaScript on websites until you specifically allow them.

As for the rest of the story on the particular email I received, forensics showed that the email originated at an IP address in Alvechurch, Birmingham, in the UK. So a UK-based computer sent spoofed email to a WV-based mail server trying to trick WV employees into clicking a link to a Polish website. Gotta love this Internet age! *Guest article by Frank Seesink (pictured) WVNET Telecommunications Network Specialist III, frank@mail.wvnet.edu*

◆ ◆ ◆ ◆ ◆ ◆ ◆ ◆ ◆ ◆ ◆ ◆ ◆



Following are a few highlights from a recently attended technology and security conference dealing with data breaches and identity theft. Conference material presented showed that approximately 10 million Americans are affected each and every year and it's just not individuals. It affects our businesses to the tune of $60 billion every year. We all need to take caution when establishing profiles on social media sites or storing personal data on our devices, especially with today's many different digital avenues, such as Facebook, Twitter, You Tube, mobile technology, laptops, etc. Once our personal information is posted or stored it may become an untouchable collection of history. For the hacker, the hunt is on for missing information they need in order to steal your identity or create a breach. The hacker is hunting for things such as passwords, social security numbers, birthdates, driver's license numbers, addresses, email addresses and credit card numbers just to name a few. We need to be aware that in the hackers' hands this information is their payday, perhaps a gold mine!

So, where do we start? Experts indicate that organizations need to first educate their employees to protect their own digital and personal reputation. Once the employees learn how to protect themselves, they can then help protect the organization with their new found knowledge. Be aware that whether we are traveling across town or the globe, anytime data leaves our workspace, the risk of theft is far greater. Protecting this information outside of the office will eliminate the single most damaging source of data theft in the workplace.

Do NOT allow any unexplainable incident to be taken lightly. A committee should be established for the purpose of examining all possible breaches and to document any new lessons learned from all unexplainable cases. It's better to be safe than sorry! The incident list may include things like: your website is overwhelmed and internet access is unavailable, slowness, divulging confidential information, loading personal and free software on work computers, weak passwords, no password expiration date, excessive login account locks, downloading, transmitting or storing sensitive unencrypted data just to name a few.

'Good privacy habits create a good bottom line.'

What defensive measures do you have in place against these types of attacks?

Here are some 'Threat Theft Tips'

Q. Do you really need all those Credit, Debit, Social Security, Insurance and Medical cards in your purse or wallet? A. No, but if you must, make a copy (front and back) of those cards so it is easier to notify the issuer in case it is lost or stolen. Be sure to store this document in an accessible, safe and secure place.

Q. How do you know if you are using a secure website for your Internet purchases, or while using online bill pay or banking? A. After selecting your site application look for '*https:*' in the URL address, this indicates that it is a Secure Socket Layer (SSL). It should turn to *green* and/or you should see a 'LOCK' icon next to the URL. If you do not see this contact the business entity and request a secure site address before entering your sensitive information. *Guest article by George Tilko (pictured) WVNET Administrative Applications SW Specialist—Senior gtilko@mail.wvnet.edu*

WVNET NETWORK OPERATORS GET NEW ROOM

WVNET's network operators will have a new room to settle into by summer of 2013. The old training lab for WVNET is being given a makeover and turned into the new Operations Room. The new room will give each operator an individual desk and have state-of-the-art monitoring of our essential systems on big screen monitors that will allow for easier and quicker recognition of problems arising within our network.

With WVNET in the process of reviewing its options for a new building, it is no secret that the last people to move into a new building will be the Operations Staff. The data center that the staff monitors will be one of the last things transferred between old infrastructure and a new building. This data center can also be used as a backup operations center once moved in the event there were a situation to occur that needed a different command center at the ready.

Operations has increased the size of its staff to 8 people in order to serve our customers more efficiently. Our staff includes:

SUPERVISORS	
Booker T. Walton III	Supervisor / Senior IT Consultant
Kimberly Jenkins	Supervisor / Senior IT Consultant
OPERATORS	
Mark Saffron	Network Operator
Barry Gregg	Network Operator
Anthony White	Network Operator
Cory Morrison	Network Operator
Michael McDonald	Network Operator
James Dubose	Network Operator

Services supported:

Telecommunications Support
Blackboard Student & Faculty Support
K-12 Email Support
Banner – Initial Response Support
Dial Up Modem Users Using WVNET Dialup
West Virginia Office of Technology After Hours Support
WVROCKS Student & Faculty Support
WV State Legislature Email Issues
RollCall Phone Conferencing Accounts
Abuse Email Filtering

WVNET's Help Desk is available 24 hours a day, 7 days a week 304.293.5192 x248

Our first Banner Users Group call for the new year was held Thursday, February 21, at 2pm. In attendance were some of our favorite people from the following institutions: *Blue Ridge CTC, Bluefield State College, Bridgemont CTC, Concord University, Eastern CTC, Fairmont State University, Glenville State College, Kanawha Valley CTC, Marshall University, New River CTC, Pierpont CTC, Shepherd University, Southern WV CTC, WV Northern CTC, WV State University, WVSOM, and WVU-Parkersburg.* That is almost 100% participation! *Maybe we can get 100% for our next call!*

wvOASIS Status: Campus finance staff have turned in their Fund and Org structure to the OASIS team. Objects and subobjects have been worked on. The state team is now working on Activity, Program/Function, and Location. There is a meeting in Charleston Mar 19 for the liaisons; generally there is a conference connection for these meetings if anyone wants to attend. The go-live date for the first phase, Budget Development, is scheduled for August 2013. While some schools have discussed entering a new chart of accounts, most are choosing to enter the new account structures future-dated in the existing chart to simplify the transition.

The invoice and manual warrant interfaces are expected to function similar to what we have now for FIMS. It is still an ongoing process. The pcard interface will change, because pcards will be reconciled in OASIS and brought back to Banner. The payroll interface will also be done this way. There is some discussion of a JV interface. For all the latest news and information, including the complete timeline of the project broken down by phase, please refer to the wvOASIS project website www.wvoasis.gov

Financial Aid Updates: The latest release is 8.16.0.4. Most schools are at 8.16.0.3. Some of the patches contained in 8.16.0.4 aren't needed by our schools. Details were sent with the patch announcement on wvbfaug-l list. Dana Keith and Dianne Sisler have been working on the shopping sheet delivered with 8.16 and have been able to get the html version to work. The PDF version is a bit more problematic but we are still working on it. The advance queuing piece is working. The next expected large release will be 8.17 scheduled for late March.

Web registration practices: One of our campuses asked the following questions as they prepare to implement web registration: *Does your institution implement PIN based registration and, if so, do you partner that with time ticketing? How does your institution handle pre-requisites? For example, Registration begins before grades are entered. Eng. 101 a pre-req to Engl. 102. What level of students are permitted to register? What student attributes do you use for restrictions? New students, special programs, etc. Are students forced to meet with an advisor before registering? Do you plan to open registration for good standing students with DegreeWorks? Did you encounter any unforeseen errors when implementing?* We would love to hear about anything else you may want to share!

Nine campuses responded that they use PIN based registration, and most use time ticketing. In progress courses are handled as fulfilling the pre-req during registration — there is a setting in GTVSDAX to turn that on. Most schools have students get their pins from their advisors; some have mandatory advisor meetings or are moving in that direction to help improve student outcomes. In some cases, some categories of students do not require pins. MU cautioned that load testing for web registration is recommended. One issue was in letting students know what sections are closed. A MU student is doing a project to build a schedule based on open sections, which could be a useful tool. For those who may not know, we have a Banner Student Listserv list that might be useful for continuing discussions on this and other topics across the state wvnsis-l@listserv.wvnet.edu To subscribe to the list, send an email to listserv@listserv.wvnet.edu with "subscribe wvnsis-l" in the body of the email.

Fine-grained Access Control—Anyone Using this? WVNCC has set up some validation tables using FGAC, and Blue Ridge has used FGAS to hide SSNs in SPAIDEN. WVNET helped set those up so we do have some limited experience with this capability.

Argos status: Lots of development is going on including conversions of reports done with Hyperion and Crystal Reports. We have Active Directory connections set up for those campuses that have AD so that campuses can easily manage their Argos user credentials. We are entitled to another week of training this year. The content of the training can be whatever we want, such as a repeat of the first training, or a quick review followed by more advanced training, and/or a workshop where everyone brings a project to work on and gets assistance from Evisions experts. We will be seeking input from our Argos users via the Argos listserv list, including best times to hold the training.

Oracle Grid Control 12c Training at WVNET April 22-24: Information was sent out to our technical users list concerning Oracle-certified training to be held at WVNET April 22-24. There are many differences and improvements with Grid Control 12c, so even those campuses who are already using Grid Control can benefit from this session. WVNET is making this class available at the discounted price of only $995, which is a real bargain compared to similar training offerings which can be more than $2000. If anyone is interested in more information that hasn't received the mailing from the BannerTechs listserv, please contact Marcie Layman marcie@mail.wvnet.edu We have several openings still available.

Banner Integration with Blackboard: WVNET is happy to be hosting nearly all of the Blackboard installations for our member institutions this year. As part of that expansion, we are offering 2 levels of Blackboard support: basic and premium. Premium support includes expanded services, which include 24 hour helpdesk support for students and faculty, expanded instructional technology and system administration support, and real-time

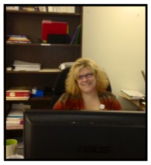
integration between Banner and Blackboard. The latter is a locally-written integration tool that uses a combination of the Banner Integration Component for initial loads with an event-driven tool that monitors Banner for web registration changes and updates Blackboard immediately. This makes it possible for a student to register for a class and immediately be able to get into the course materials on Blackboard instead of waiting for the next day. Those campuses interested in setting up this integration should submit an Oz ticket and we will get you on our list.

DegreeWorks Status: We have a number of outstanding issues with Ellucian that have caused delays in production implementation of DegreeWorks for the first group of schools. Some of these are software defects that we are working with the support center to resolve, and some are due to unresolved training issues. The second group of campuses are well into their implementations now, but are also experiencing challenges due to the unresolved issues from the first group. WVNET has arranged with Ellucian to get some additional consulting support to get these issues resolved and the backlog caught up. Marshall noted that while they are in full production for approximately half of their undergraduate students, they saw approximately a 30% overrun on consulting hours over the original estimate. The WVNET groups have also used more hours than the original estimates, though maybe not quite that much in most cases.

Next Banner Users Group Call (third Thursday) is March 21 at 2.

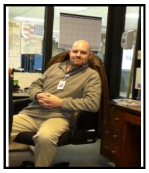
WVNET Volunteers at Work: Seemingly, all things have data and computers. As many people volunteer in different ways, WVNET's own Dana Keith spends his extra time to use both his computer skills and his sporting interest in swimming to be the meet coordinator for the *West Virginia Secondary School Activities Commission State Swimming Championships*. Keith has done this for the last seven years after serving as Assistant Swimming Coach at University High School from 2001-2006. *"The computer is a tool to allow us to take the top swimmers from each of the West Virginia four regional meets and build a program of the top 24 swimmers in the 22 boys and girls events. It is exciting to see the improvement each year in the swimming programs and I am glad to have the knowledge and time to help with this event."* This year's meet was hosted at the WVU Natatorium where three hundred high schools competed, with results including three national time qualifying swims. ***GO DANA!!!***

PERSONNEL NEWS



LaVonne Doljak joined the WVNET Business Office staff as *Accounting Assistant II.*

Bridgette Boyd, a senior Political Science major at WVU joined the WVNET Business Office Staff as a *Student Worker*. Bridgette will be helping out with a variety of business office tasks.



James DuBose began work as a *Network Operator*. James holds an Associate Degree from West Virginia Junior College but his degree is in Network Software Solutions. Most recently, he has been a PC technician at My Radio Network but he also spent four years in the US Army where he lead a team of networking professionals.

Michael McDonald (not pictured) began work as a *Network Operator*. Michael comes to us from TeleTech where he has gained excellent customer service experience. He also has an Associate Degree in Information Technology from West Virginia Junior College.

Fran Barnes has joined the WVNET Media Services team as *Editorial Assistant* where her responsibilities with the newsletter and branding are a better fit.

Karen Saffron has joined the WVNET Media Services team. As the WVNET conferences have evolved, Karen has spent substantial time working in tandem with Media Services, so much so that it is now appropriate for her position to be housed there.

Mike Karolchik has returned fulltime to WVNET where he serves as *Manager of Media Services*.

Sam Lay (Blackboard support) left WVNET's employ recently however, not to worry, we have *whiz kid Jonathan Lynch*!!

West Virginia NETWORK
Enhancing Education through Technology

Dan O'Hanlon, Director
837 Chestnut Ridge Road
Morgantown, WV 26505
304.522.7303
dohanlon@mail.wvnet.edu

Fran Barnes, Editorial Assistant
fran@mail.wvnet.edu

Fran Barnes

follow us on twitter

Follow @ wvnet

Newsletter Archives Here
www.wvnet.edu

From the Director…

Things are always interesting at WVNET these days. We have interns and work study students who bring a lot of energy and talent to our offices. They work in nearly every group inside WVNET and it is always interesting to hear what they are doing to make things better for us and for our customers.

> We have them working on updating our website, making Disaster Recovery easier and quicker, making reports a lot simpler to pull out of Banner for our schools, even working in our Business Unit to make the way we pay our bills smoother and better.

> We understand that many of you out there work with students every day in our Universities, Community & Technical Colleges, and K-12 schools. But for WVNET, we were without students for many years.

> Having them back reminds us of why we all get up and work so hard each day because young people truly are our future, at WVNET and in West Virginia! —*Dan O'Hanlon*