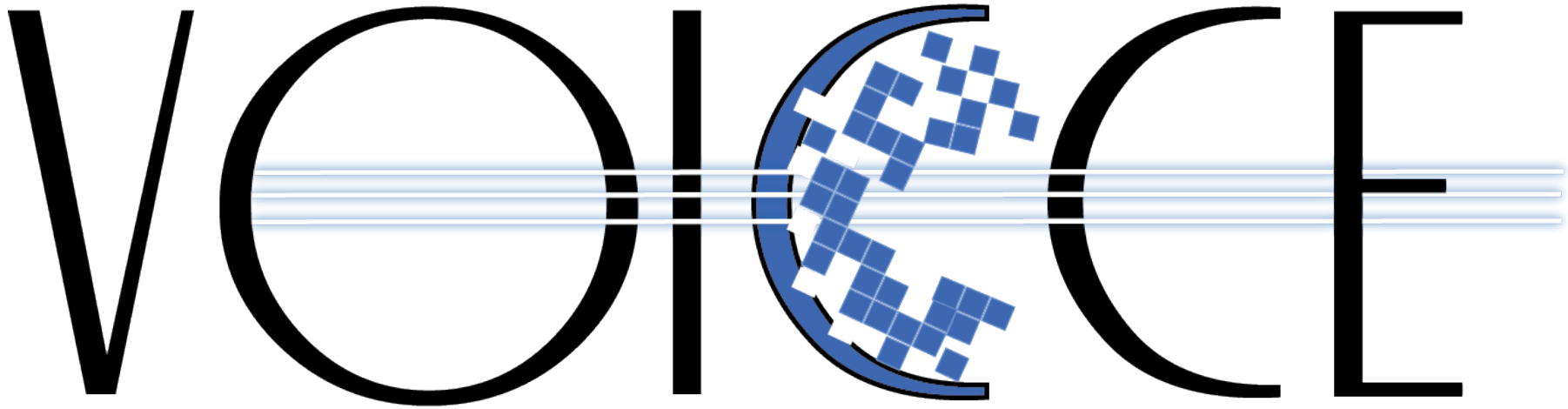


Virginia's Operational Integration Cyberspace Center of Excellence

CYBER SECURITY PRACTICES TO COUNTER FRAUD

April 23rd, 2012

ZelTech®
Zel Technologies, LLC

Overview

- Introduction
- Cyber Threat Landscape
- Cybercrime Activities
- Best Practices

Intro - ZelTech & Cyber Security

- **ZelTech has 15+ years experience providing information security and compliance expertise to federal, state, local and commercial entities. Customers include the DoD, DHS, Intel Agencies, VPA, Hampton, and VOICCE.**
- **Initial contracts were at the federal level and included:**
  - Network architecture and modernization planning, security engineering, and policy management.
  - Day-to-Day Network and Security Management of highly critical and sensitive worldwide networks.
  - High end Research and Development, primarily focused on risk management.
- **ZelTech later leveraged our federal experience for state, local and commercial clients including VOICCE, the Nation's first municipally-oriented Cyber Center of Excellence. Efforts include:**
  - Network design and server management.
  - Policy development and enforcement.
  - Vulnerability and Risk Assessments.

VOICCE

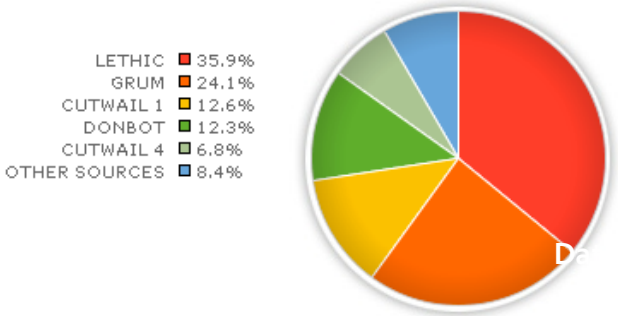
- **VOICCE is a non-profit activity focused on improving cyber security at the local level. Key tasks include standing up a municipal cyber lab to evaluate:**
  - Cyber response planning and training
  - Identify and evaluate appropriate policies and affordable tools
  - Support models for cyber security analysis and response planning
- **Provides an environment to create a "virtual municipality" for training, evaluations and experimentation**
- **Municipal Lab**
  - Continually enhanced cyber lab
    - Modeling tools installed and models continuously under development
    - Models enhance understanding and policy development and effectiveness
    - Open Source NOC/SOC developed and can be deployed or used remotely
    - Additional tools and capabilities being procured and evaluated
  - Supports
    - Cyber response exercises and evaluations
    - Information sharing
    - Cyber training, awareness, and workforce development

Cyber Threat Landscape

- **Cyber threats are evolving**
  - In the past, many threats were static, easy to identify and could be defeated using firewalls and "virus checkers"
  - Many attacks were noisy, focused on web site defacement, denial of service or single tasks like stealing passwords
- **Today's threats are far more sophisticated, targeted and toolsets are available to the public and organized crime**
  - Today's threats are stealthy, persistent and hide/promulgate across multiple devices and in general network traffic
  - Firewalls are important to protect critical networks but public facing applications provide a wide variety of attack vectors
  - Malware targeted against specific environments and designed to exfiltrate key data, primarily for financial gain
- **Increased dependence on mobile devices increases the attack surface and provides new ways to compromise critical systems through trusted relationships**
- **Regardless of the specific attack vector, the most common tactic is based on stealing user credentials using technical and social methods.**

Advanced Threats

- **Advanced threats use a highly highly distributed infrastructure (botnets) to support very organized criminal organizations.**
  - Huge amounts of sophisticated Spam, managed by relatively few "owners" target users either very broadly or very specifically (i.e., spearphishing).
  - "Clicking" on malicious links or "drive-by" attacks on poisoned websites load malware (mostly trojans) on victim computers.
  - Data is harvested and sold to highest bidder.



- **APTs can use either approach to infect computers with active agents that "call home" to C2 servers and pass data. In addition, agents propagate across networks with many agents remaining dormant until required.**
  - Botnets are highly decentralized but C2 nodes increasing their decentralization.
  - This is "big business" whether is designed to steal intellectual property, harvest credit cards and personal information.
- **Threats can result in direct monetary or IP thefts but also significant financial losses due to credit insurance costs, loss of customer confidence, and other related business impacts.**

Mobile Environment

- **Mobile access growing rapidly and 2011 showed both the largest number of attacks and growth in mobile malware in history. Vulnerabilities include:**
  - Routine lack of any security software.
  - Increasing number of unvalidated application downloads.
  - Trusted relationships with enterprise and financial systems.
  - Data leakage includes credentials, contact lists, location data, etc.
- **Even sophisticated users trust their phones much more than Spam on their computers (which tend to have more protection).**
  - "Smishing" is a growing threat and users that would never respond to an unexpected e-mail will provide personal data to a text or voice message.
  - Other attack vectors include using voice mails ("vishing"), Twitter, and social networks.
- **Mobile technology is not as advanced and not normally managed.**
  - Browsers tend to be much less secure and prone to poisoning.
  - Due to rapid market cycle; operating systems, browsers and app software not routinely updated or patched.
  - Mobile devices also exposed to threats over both 3/4G networks but also open and protected WiFi systems.
- **As a result of these threats, mobile phone vulnerabilities affect not only users but also the enterprises they support. Many experts predict even more growth in mobile attacks in 2012.**

Cybercrime Activities

Banking and ACH Scams

- **Bank Scams – Attempt to acquire financial assets from people and organizations. A 2011 survey by Ponemon Institute and Guardian Analytics highlighted how vulnerable SMEs were:**
  - Out of 500+ companies surveyed, 55%+ were defrauded in previous year.
  - Over 60% involved online bank fraud and over half were attacked more than once.
  - Over 87% failed to recover lost funds and ~80% detected frauds after transfer.
- **Attacks usually leverage credential theft using technical and social methods.**
  - FDIC & Patriot Act. In 2011, bogus emails claimed FDIC & DHS had removed insurance due to "suspected violations of Patriot Act." Emails had links that downloaded malware to harvest user names, financial data and passwords that were used to transfer the funds.
  - Social Networks. Multiple cases in 2010/11 that included asking "coworkers" over FB or Twitter for log in data to do work that had to be done over the weekend. Funds were transferred and lost over weekend. Other cases use "friends" infect computer.
- **Basic Flow:**
  - Authorized employee logs on to online account from infected computer.
  - Malware captures credentials.
  - Criminal logs on account and transfers funds to multiple accounts. This transfer at times may include a DDoS aspect to delay reactions.
  - Money mules process transfers, usually sending money overseas. Very recent reports suggest tendency to move from mules to prepaid credit card accounts.

Cybercrime Activities

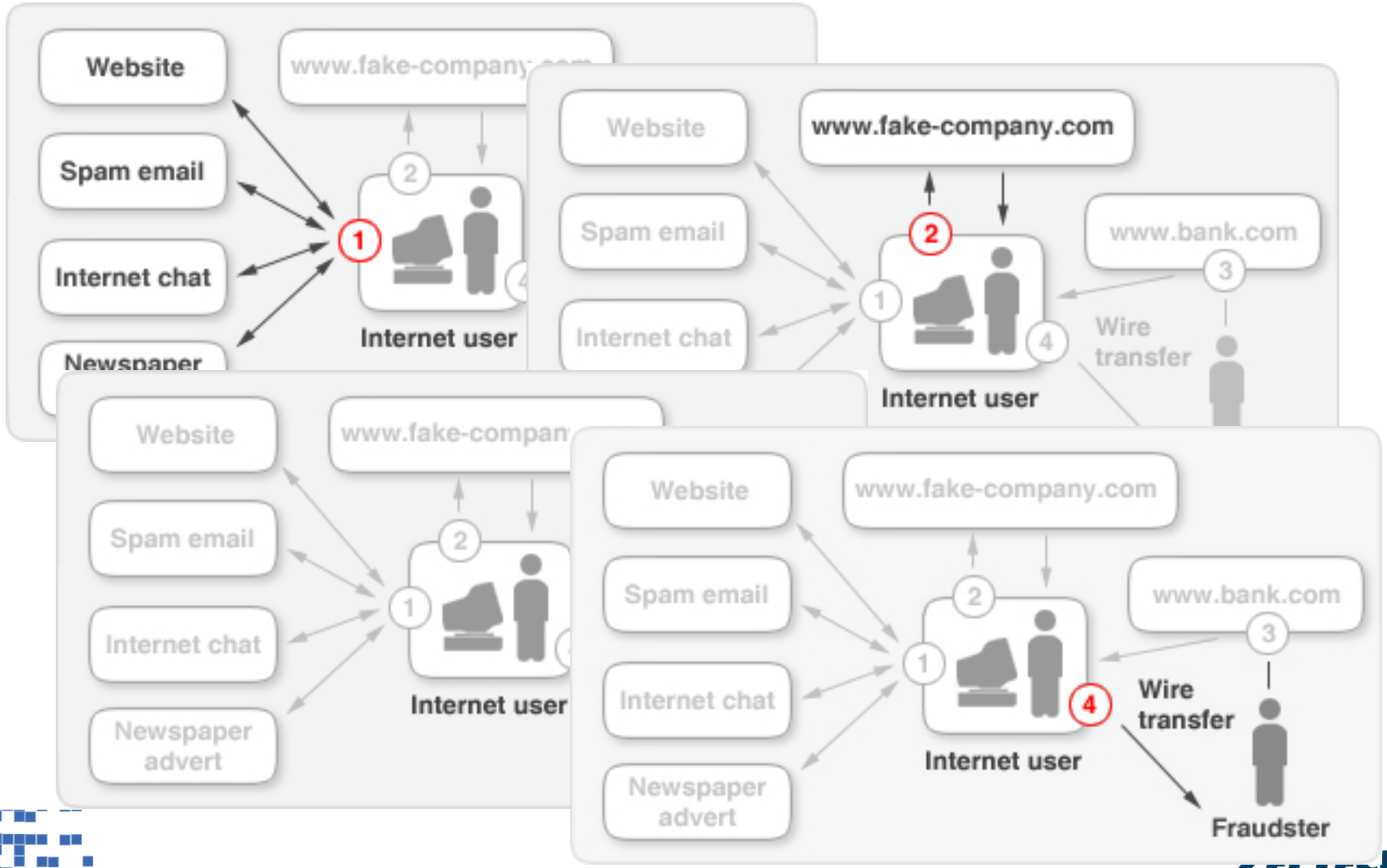
Example ACH Scams

- **Sign Designs, Modesto, CA.** Zeus Trojan allowed company computer to access its accounts and transfer ~$100K to 17 mules at 7 banks around US.
- **Bullitt County, Ky.** Zeus variant sent credentials via IM and provided a backdoor for criminals in Ukraine.
  - Treasurer's email and passwords were changed
  - Created 25 fictitious employees (mules)
  - When criminals logged in with "wrong" IP, bank detected change and sent validation challenge
  - Crooks responded and effectively approved $415K of transfers to mules.
- **Alta East, Middletown, NY.** March 13, 2012. Four workers received emails from "client" with questions about a recent invoice that was "attached", infecting their systems and resulting in $121K loss.
  - March 19, six payments to fake employees were sent to 15 Metabank accounts. Additional 15 transfers sent to traditional mules around the country.
  - Provident Bank notified Alta East late that day but not responded to until next day – most transfers had already been processed.
  - Approximately $40K recovered.
  - Alta East IT staff scanned Comptroller's computer with six different AV tools, nothing found (Trojan isolated with specialized tools).

```
!!Details of our 1 client:

*NOTE* (!!!PLEASE PAY WESTERN UNION TRANSACTION FEES FROM $3073 USD!!!!!)
FIRST NAME:  Valeriy
SURNAME:     Zobnin
CITY:         Poltava
COUNTRY:      Ukraine


!!Details of our 2 client:

*NOTE* (!!!PLEASE PAY WESTERN UNION TRANSACTION FEES FROM $3073 USD!!!!!)
FIRST NAME:  Andrey
SURNAME:     Kostin
CITY:         Rovno
COUNTRY:      Ukraine

!!Details of our 3 client:

*NOTE* (!!!PLEASE PAY WESTERN UNION TRANSACTION FEES FROM $3073 USD!!!!!)
FIRST NAME:  Boris
SURNAME:     Valinurov
CITY:         Kiev
COUNTRY:      Ukraine
```

Cybercrime Activities

Example Fraud Flow



Best Practices
Secure Your Environment

VOICCE
Virginia's Operational Integration Cyberspace Center of Excellence

- **Secure your business and its connections with policies and technology.**
  - Develop an overall security program and required policies.
  - Users should have different accounts and passwords. Restrict rights to those needed for their jobs. Not everyone needs admin rights!
  - Install firewalls and encrypt all wireless access (at work and at home) with at least WPA. Control computer access and especially on laptops and mobile devices, consider encryption.
  - Keep operating systems, applications, and security software up-to-date.
- **Train your people to be extremely careful opening attachments, even when you believe you know the source. Watch out for Spam and Spim.**
  - Stop – Think – Connect
  - Many attacks require an attachment on email, social media, etc be opened.
  - Not all users need to install software or have "admin" rights!
- **Back up your files and preferably keep the back-ups offsite.**
  - Consider encrypting most sensitive data, especially on laptops.
- **Set-up safe web site browsing rules and consider restricting web access to most sensitive computers (i.e., credit card or finance processing).**
  - Anytime you are buying/selling online or working with your bank, make sure the url is "plural" (i.e., https vs http), especially if mobile.

ZELTECH®
Zel Technologies, LLC

First Line of Defense
Passwords

- **Passwords**
  - Many passwords are ineffective and easy to guess (abc123, names backwards, pet names, etc.)
  - Make them easy for you to remember but hard to guess. Use capital letters, numbers and symbols.
  - Don't write them down, especially in your laptop case.
  - Deploy a solid password policy and enforce it with technical means.
- **Password Resets are typically done via secret questions and email to preferred email account such as:**
  - Mother's maiden name?
  - Father's middle name?
  - Favorite pet's name? …
- **Conundrum**
  - Real answers easy to remember but discoverable via Google, facebook, etc.
  - False answers harder to remember but safe from online searches.
- **Treat your "secret questions" as seriously as your passwords**
  - Never share either and change them often.
- **Consider using a password manager.**
  - Examples include LastPass, 1Password, RoboForm, Wallet, Sticky Password, etc.

Secure Mobile Devices

- **Mobile devices and smart phones are becoming a standard, contain a lot of sensitive information, and often have trust relationships with work and home networks.**
  - They are rapidly becoming an attack vector and must be secured.
  - Most people think before they click on the computer but we trust our smart phones.
  - Focus on protecting credentials.
- **Eight Key Essential Steps**
  - Lock your device and consider a "self-destruct" setting.
  - Evaluate use of mobile security software such as Lookout™, Kapersky, McAfee, PRTGdroid, Webroot, Trend Micro, AVG, etc.
  - Require ability to remotely "wipe" any mobile device with sensitive data.
  - Avoid new and questionable apps.
  - Update the operating systems and apps.
  - Back up your data.
  - Carefully consider security implications before "jailbreaking".
  - Understand the smishing, Twitter, and voice mail attacks.
  - **STOP.THINK.CONNECT** on your phone too.

Website and Email Security

- **Web server & web site security are critical to a company's overall security posture and are often primary targets for cybercrime.**
  - Carefully plan and address security aspects for your website and any blogs. Consider splitting your public website from a secured website for employees.
  - Carefully evaluate information required on public website, its the first place criminals will go to plan an attack. More complex sites have more risks.
  - Ensure required security and compliance requirements are documented and audited. Commit to an ongoing security maintenance approach.
- **Email security is critical because it provides a way to attack the company through any employee or activity, not just "through your firewall."**
  - Develop an email usage policy and train your employees in its requirements. Email is insecure and any sensitive data (e.g., PPI, PHI, sensitive data, etc) must be controlled.
  - Implement an appropriate email retention and control policy that meets or exceeds any compliance or regulatory requirements for your business.
  - Carefully evaluate requirements for email on mobile devices (company or employee owned). Mobile devices with trusted relationships with the business should meet security requirements and rules (locks, remote wipe, etc).
- **Consider outsourcing web site and email services to a reliable vendor.**
  - Ensure that vendor complies with required standards (PCI, HIPAA, FISMA, etc) and keeps website software up to date.

Scams and Fraud

- **Train employees to recognize social engineering, phishing whether asking for information or "clicking" on links.**
  - Approaches can include contacting employees online, via telephone, cell phone/SMS, or in person.
- **Protect your company and customers against online fraud.**
  - Carefully inventory data and only store what is required to be online.
  - Consider outsourcing online payments to limit data loss liability. PCI/DSS compliance is expensive but data loss is even more expensive!
- **Protect against malware and fake antivirus software.**
  - Anti-malware software is not the same as traditional antivirus, get both.
  - Train employees recognize real warnings & not to click on others.
  - Consider not giving all users admin rights so it is harder to install malware.
- **Consider a stand-alone computer for all routine financial transfers.**
  - Register IP address with banks and ACH network.
  - Evaluate use of multifactor authentication.
  - Consider use of "Live" CD to boot this computer.

"Take-Aways"

- **Attack techniques are changing.**
  - Less dependence on traditional "viruses".
  - More attacks use Malware and Phishing attacks.
  - Protect against both.
- **Over 90% of the attacks are thwarted by basic hygiene and common sense so:**
  - Think before you connect.
  - Keep operating systems, anti-virus and malware checkers up to date.
  - Use strong passwords and change them often.
- **Less than 10% of the attacks are very sophisticated and expensive to detect and defend.**
  - Most individuals are simply not that attractive a target.
  - The most sophisticated adversaries go after the federal government, DoD contractors and large businesses.
  - Targeted attacks on small and medium-sized businesses are increasing rapidly.
  - Attacks on municipal governments are growing.
  - For academia, if you aren't protected, you are providing free R&D to our enemies.

Summary

- **For most of us, cyber security doesn't have to be expensive or overly complicated but it does have to be intentional. Attack techniques are changing.**
  - Less dependence on traditional "viruses".
  - More attacks use Malware and Phishing attacks.
  - Protect against both.
- **Over 90% of the attacks are thwarted by basic hygiene, common sense, and planning so:**
  - Think before you connect.
  - Ensure passwords are updated and never keep default passwords or broadcast IDs
  - Keep operating systems, anti-virus and malware checkers up to date.
  - Use strong passwords and change them often.
- **Secure your environment with a firewall and encrypted wireless access points. Evaluate what info needs to be public or accessible through the web or on mobile devices.**
- **There are a number of online assets that help to understand threats and maintaining your security.**
  - The VOICCE website at http://www.voicce.net links to a number government, non-profit, and commercial sites. It also contains a variety of papers, videos, and reports to help local government, academia, businesses, and citizens.
  - If there are questions that need to be answered, please provide feedback and we will try to support your requests.

Cyber Security Information Assets

- VOICCE – http://www.voicce.net
- Multi State – Information Sharing and Analysis Center – http://msisac.cisecurity.org
- DHS Cyber Security – http://www.dhs.gov/files/cybersecurity.shtm
- STOP.THINK.CONNECT – http://stopthinkconnect.org
- DHS STC Campaign – http://www.dhs.gov/stopthinkconnect
- US Computer Emergency Readiness Team – http://us-cert/gov
- US CERT Cyber Security Tips – http://www.us-cert.gov/cas/tips
- Virginia Information Security Tips – http://vita.virginia.gov/communications/publications/InformationSecurityTips
- FCC Small Business Tips – http://www.fcc.gov/cyberforsmallbiz
- Cyber Watch Center – http://cyberwatchcenter.org/
- InfraGard – http://infragard.net
- Internet Crime Complaint Center (IC3) – http://www.ic3.gov/default.aspx
- Symantec Security Focus – http://www.securityfocus.com/
- Stay Safe Online – http://www.staysafeonline.org/
- Anti Phishing Working Group – http://www.antiphishing.org/
- Technology & Marketing Law Blog – http://blog.ericgoldman.org
- Bank Info Security – http://bankinfosecurity.com
- Krebs On Security – http://krebsonsecurity.com/
- M86 Security Lab – http://www.m86security.com/resources/
- Dark Reading, Protect the Business – http://www.darkreading.com/

Bruce Sturk, Executive Director, VOICCE, bsturk@hampton.gov
Scott Arnott, Technical Director, VOICCE, sarnott@zeltech.com