Tech Update and Email
Tech Update

Last Semester:
- Installed DR4300 Disk Backup System
- Purchase Thin Client Computers
  - Westec Classroom
  - G3 and G4 Classrooms
- Added TVs to G8,9,10 with DVD player
- Upgraded older computers with SSD Drives
- Looking at computer to projector interface
- Review MS Forms available in your Email
- Launched Canvas automated upload
Archive has changed to 1 year!

Per Dr. Daniels we have changed archiving to one year for Faculty and Staff! Changed in December and still in my inbox.

3CBG Chief Technology Officers

Daniel Watkins

Hello All, Please see attached Agenda and Minutes for...

If you didn't find what you were looking for, try again using more specific search terms.
Microsoft Modules
Information Security and Email

Are you the only one accessing the computer?
How safe is your information?
What to look for when shopping on the Internet?
Are websites dangerous?
What can you do?
At home or work

- Separate accounts
- User name and passwords
- Password protect your documents
- Backup your work
- Watch out for strange problems
- Look for traffic on cable modems
- Update patches for Microsoft Products
Who is lurking about?

- Computer Hackers
- Script Kiddies
- Virus Writer
- Spam Mail
- Sniffers
- DDoS Denial of Service
- Phishing Attempt
- Ransomware
Old Style

Download the First Class® 7.1 Client here: Download

Download the First Class® 7.0 Client optional files here: Windows  Macintosh

Download the First Class® 7.0 Client personal files here: Windows  Macintosh

Download the First Class® Extensions for Palm OS  Windows  Mac OS  Mac OS X

For technical support please contact:
New Style
Spammers – Email Viruses

- Information leakage & loss
- Spreading the Virus
- Un-ending junk mail

The World's Worst Spammers

Up to 80% of spam targeted at internet users around the world is generated by a hard-core group of around 100 known persistent spam gangs whose names, aliases and operations are documented in Spamhaus' Register Of Known Spam Operations (ROKSO) database.

This TOP 10 chart of ROKSO-listed spammers is based on Spamhaus views of the highest threat, least repentant, most persistent, and generally the worst of the career spammers causing the most damage on the internet currently.
The 10 Worst Spammers

As of 13 January 2017 the world's worst spammers and spam gangs are:

1. **Canadian Pharmacy** - Ukraine
   A long time running pharmacy spam operation. They send tens of millions of spams per day using botnet techniques. Probably based in Eastern Europe, Ukraine/Russia. Host spammed web sites on botnets and on bulletproof Chinese web hosting.

2. **Dante Jimenez / Aiming Invest** - United States
   Spamwarez, lists, "bulletproof" hosting in the finest South Florida tradition. Working with worst cybercriminal botnet spammers. Now mostly involved in massive botnet spamming with hosting on hacked servers and Eastern European hosts.

3. **Yair Shaley / Koheni Solutions** - United States

4. **Michael Lindsay** - United States
   Lindsay's iMedia Networks is a full-fledged spam-hosting operation serving bulletproof hosting at high premiums to well known ROKSO-listed spammers. His customers spam via botnet zombies with spam payloads hosted offshore, tunneled back to his servers. He and the gang have been hijacking (stealing) IP address space from companies for years to spam from. Illegal in the USA.

5. **Michael Boehm and Associates** - United States
   Snowshoe spam organization that uses large numbers of inexpensive, automated VPS hosting IPs and domains in whatever TLD is currently cheapest to send high volumes of spam to extremely dirty, scraped lists. Operates under many business and individual names.

6. **Peter Severa / Peter Levashov** - Russian Federation

7. **Yambo Financials** - Ukraine
   Huge spamhaus tied into distribution and billing for child, animal, and incest-porn, pirated software, and pharmaceuticals. Run their own merchant services (credit-card "collection" sites) set up as a fake "bank."

8. **Michael Persaud** - United States
   Long time snowshoe type spammer, recently raided by FBI.

9. **Alvin Slocumbe / Cyber World Internet Services** - United States
   Bulletproof spam host operating Cyber World Internet Services / e-Insites, and currently spamming using a variety of aliases such as Brand 4 Marketing, Ad Media Plus, Site Traffic Network, RCM Delivery, and eBox.

10. **Jager Babuin / BHSI** - Canada
    Romanian spammer now living in Vancouver BC. Also known as the "Dr Oz" spammer.
Got an Email from Somebody You don’t know?

This is not taftcollege.edu

-------- Original message --------
From: Administrator <admin@mpbentong.gov.my>
Date: 1/11/17 14:13 (GMT-08:00)
To: 
Subject: Validate your e-mail address

Dear Staffs,

Your Account information needs to be updated within 24 Hours, If this is not done we shall suspend your account.

Please Click Here to Update: http://emailactivationdatabase2017.hexat.com/index

Thanks for your understanding and Co-operation.

System Management Team.

------------ ITS staff will use their signature, don’t know don’t trust, call and check! ------------
Hacked Email, Yahoo anyone?

Sign up with any service online, and it will almost certainly require you to supply an email address. In nearly all cases, the person who is in control of that address can reset the password of any associated services or accounts—merely by requesting a password reset email.

Your email account may be worth far more than you imagine.
Your infected! What happens?

Next time someone asks why miscreants might want to hack his PC, show him this diagram.
What to do!

- Password protect files
- Install a home firewall if you have Roadrunner or DSL
- Be careful to open email without subject headings
- Check to see if email is from the Internet
- Delete questionable email before opening it
- Use MacAfee or Norton's Antivirus
Now a story! Ransomware

Los Angeles Valley College Pays a Whopping $30,000 in Ransomware Incident
bleepingcomputer.com · 3 days ago
"Merry Christmas" Ransomware Now Steals User Private Data via DiamondFox Malware MongoDB Apocalypse: Professional ...

Los Angeles Valley College Pays US$28,000 In Bitcoin After Ransomware Attack
livebitcoinnews.com · 1 day ago
Ransomware attacks remain a constant threat to our society, even in 2017. The Los Angeles Valley College was forced to pay US$28,000 ...

Community College Pays Hacker $28,000 for Ransomware ...
https://campustechnology.com/articles/2017/01/10/community-college... ▼
Jan 10, 2017 · Los Angeles Valley College (LAVC) is investigating a ransomware attack that took place last month, forcing the California Community College system to ...
Community College Pays Hacker $28,000 for Ransomware Attack

By Staff | 01/10/17

Last month, Los Angeles Valley College (LAVC) was hit with a ransomware attack, forcing the California Community College system to pay an unidentified hacker nearly $28,000 to retrieve stolen data. The investigation is still in the early stages, and as of now no breach data was identified.

LAVC consulted with its leadership, outside cybersecurity experts and law enforcement before making the payment. “It was the assessment of our outside cybersecurity experts that making a payment would offer an extremely high probability of restoring access to the affected systems, while failure to pay would virtually guarantee that data would be lost,” according to a statement. The attack has disrupted many computer, online, e-mail and voicemail systems.

The United States Department of Justice estimates that approximately 4,000 ransomware attacks occurred every day in the U.S. in 2016. Education is the sector most targeted by ransomware, according to a recent report from security analyst BitSight, which found that 13 percent of institutions experienced ransomware attacks last year.
LAVC Cybersecurity Event Frequently Asked Questions

LATEST UPDATE (January 6, 2017):

Did LAVC pay the ransom?
In consultation with district and college leadership, outside cybersecurity experts and law enforcement, a payment was made by the District. It was the assessment of our outside cybersecurity experts that making a payment would offer an extremely high probability of restoring access to the affected systems, while failure to pay would virtually guarantee that data would be lost.

Did it work?
After payment was made, a 'key' was delivered to open access to our computer systems. The process to 'unlock' hundreds of thousands of files will be a lengthy one, but so far, the key has worked in every attempt that has been made.

How did we pay for it?
The District has a cybersecurity insurance policy to address these specific types of cyber intrusions and it was activated during this incident. While much time will pass before this matter is resolved, we have already availed ourselves of the resources provided by the policy, including assistance of cybersecurity experts.
Does it happen here!

Yes it can at any time, are any devices safe? No!

Will this cause us to be more stringent? Yes!
Strong Passwords, More Procedures and Plans!

Disaster Recovery Plan
Data Security Plan
More Backup Plans
Research Links

- [www.sarc.com](http://www.sarc.com) – email virus and hoax alerts
- [www.symantec.com](http://www.symantec.com) – software-antivirus-firewall
- [www.mcafee.com](http://www.mcafee.com) – antivirus software
- [www.zonelabs.com](http://www.zonelabs.com) – firewall software
- [www.checkpoint.com](http://www.checkpoint.com) – industrial software
- [www.firewallguide.com](http://www.firewallguide.com) – info guide on products