District IT Security for Staff

Richard Harlin
Microcomputer System Director
May, 2010

Scope of Presentation

- Email Security Issues
- Security of Systems and Files
- Privacy and File Management

Email – Restricted Activities (District Regulation)

- The creation and exchange of improper messages. Email should follow the same standards expected in written business communications and public meetings.
- The exchange of proprietary information or any other privileged, confidential information without a warning regarding accidental transmission to an unintended third party.
- The creation and/or exchange of unsolicited commercial e-mail (SPAM).
- The creation, distribution, transmission, access, or other use of any material in violation of Federal or State Law is prohibited.
- Registration to list servers without proper authorization is prohibited.
- Exchange of messages directly impacting the performance of the e-mail system.
- Reading or sending messages from another user's account except under proper delegate arrangements.
- Altering or copying a message or attachment belonging to another user without the permission of the originator.
- Compromising the privacy of email or you email password by giving it to others or exposing it to public view.

Email Security and SPAM – Avoiding fraudulent email

SPAM is unwanted mass-marketing E-Mail. The vast majority of SPAM messages coming into the District are filtered out at DCBOCES, but a small percentage still get through. Some are marked as [SPAM] in the email title by the system.

In general, if it sounds too good to be true, odds are it isn't true:

- **You have not won the Irish Lotto, the Yahoo Lottery, or any big cash prize.**
- **There is no actual "Nigerian" King or Prince trying to send you $10 million.**
- **Your Bank / Credit Card / Membership / Email Account Details do not need to be reconfirmed immediately, online.**
- **You do not have an unclaimed inheritance.**
- **You never actually sent that "Returned Mail".**
- **The News Headline email is not someone actually informing you about daily news.**
- **You have not won an iPod Nano / Computer / Free Trip / House, or WHATEVER.**
- **"FWD: Your computer may be infected!" It isn't…….**

Email Security and SPAM – Avoiding fraudulent email (Phishing)

Avoiding PHISHING mail:

- The goal is to fool you into entering your information into something which appears to be safe and secure, but in fact is just a dummy site set up by the scammer.
- Providing the phisher with personal information will allow them to steal your identity and your money, or to spam others.
- Signs of phishing may include:
  - **A logo that looks distorted or stretched.**
  - **Email that refers to you as "Dear Customer" or "Dear User" rather than your actual name.**
  - **Email that warns you that an account of yours will be shut down unless you reconfirm your billing information immediately.**
  - **An email threatening legal action.**
  - **Email coming from an account similar to, but different from, the one the company usually uses.**
  - **An email that claims 'Security Compromises' or 'Security Threats' and requires immediate action.**

Email Security – Some Simple Solutions

1. **Keep your passwords/personal information to yourself:**
   - **There is no "lost information"**
2. **Verify the sender:**
   - **Call or email them back – ask questions**
3. **Don't open attachments w/o verification**
   - **If you get malware, notify IT ASAP**
   - **Beware of files ending in .exe, .com, .zip, .dll – do not open**
4. **Don't click on links w/o verification**
   - **You can "hover over" the link to see where it goes**
5. **Don't leave your system unattended with email up**
6. **In Outlook, Add the Sender to the Blocked Senders List**
7. **In Outlook, Create a Rule.**
8. **Check Recipients before Sending.**
   - **Be careful of "all" sending**

Security of Systems and Files – (District Regulations)

1. No user may access or attempt to access information on District technology assets without proper authorization and legitimate authentication.
   - **No one should be logged in under another user's credentials for normal activities**

2. No user may perform any action which has the effect of disrupting District business.
   - **Deletion or alteration of another user's files**
   - **Storage of non-work related materials**

3. Staff members are responsible for insuring the security of any technology assets assigned to or created by them.
   - **Use care and caution when using the Internet**
   - **Passwords should be changed if it is suspected that they have been compromised, by contacting the network coordinator (form on web site)**
   - **Do not relocate equipment without permission (form on web site)**
   - **Notify IT if you suspect a virus or malware infection**

4. While signed into the network, a staff member may not leave any workstation unattended and in an unsecured state at any time.
   - **Lock up equipment when unattended**
   - **Do not leave equipment logged in and unattended**

5. Staff members with access to student records may not use, share, or release such records except as authorized by the District and/or State and Federal law.

Security/Privacy of Files – (Public Regulations)

Regulations pertaining to files and emails:

1. FERPA – Family Educational Rights and Privacy Act
   - Under FERPA, schools must generally afford parents:
     - access to their children's education records
     - an opportunity to seek to have the records amended
     - some control over the disclosure of information from the records.

2. FOIL – NYS Freedom of Information Law, under which emails, files, and other communications my be requested by members of the public.

Other Regulations:

CIPA - Children's Internet Protection Act, limits children's exposure to pornography and explicit content online. We comply through active filtering of explicit web sites.

Privacy and File Management on the PPCSD Network

Network Storage Areas:

- Structure in effect since 1998
- Storage areas are assigned access rights by the login name and password.

1. Drive “G:” – Drive letter assigned to person logging in, “personal drive”
   - For Staff members, only the user and the network administrator have access
   - For Students (HS/MS uses unique logins), the Student, Teachers, and the Network Administrator have access to the individual Student folder.

2. Drive “J:” – Drive letter assigned to teaching staff by building, “Teachers Common Drive” one for HS/MS, one for SS, one for CS
   - Teaching Staff has read/write access, Students have no access.

3. Drive “K:” – Drive letter assigned to teaching staff and students, “Student Common Drive”
   - In the HS/MS, Teaching Staff has full read/write/erase access, students have read-only access.
   - In the Elementaries, both Teaching Staff and Students have read/write access.

Privacy and File Management on the PPCSD Network (2)

Caution needs to be exercised when saving files of a confidential nature on the network drives:

- Drive G: is the personal drive of the person logged in; hence, you would not want to save a confidential file there if a student is logged into that computer. If you are not sure who is logged into a particular machine, log out and then log in as yourself, or look in MY Computer, the G: drive will have the login name of the person currently logged in attached to it.

- Never save confidential files to a Student's personal save area.

- Drive J: is accessible to all teachers in a particular building, but not to students. It is generally safe to use, but a teacher needs to exercise caution not to erase or change another teachers work.

- Drive K: is OFF-LIMITS for any confidential file, personal files, or communications, since it is Student accessible. Do not save any files to this area that are not intended for student use.

If you have questions about any of the subject matter covered here, please feel free to contact the Information Technology office at HS X417 or X407.