Keeping Your Data Safe

John Roberts
Director of Computer Systems and
Chief Information Security Officer

Security is everyone’s responsibility!
Keeping Your Data Safe

Today’s Topics

• Why we need to know about data security
• Teachers and administrators and data security
• Safe computing practices for everyone
• Resources
Why we need to know about data security

Teachers and administrators --- **Must comply** with legal and regulatory requirements

**Everyone** --- To protect personal data from exposure and malicious attacks
What is data security?

Data security is the practice of keeping data protected from unauthorized access and corruption or loss.
Computer and Data Security

Today’s Topics

• Why we need to know about data security
• Teachers and administrators and data security
• Safe computing practices for everyone
• Resources
Why we need to know about data security – What are the risks?

For teachers and administrators

- Identity theft
- Violation of federal/state/school system regulations
- Damage to the school/school system reputation and subsequent loss of public trust
- Civil action and fines
- Loss of the ability to do business

For everyone

- Identity theft
- Financial loss
- Personal exposure
Teachers and Administrators
Regulatory Requirements - Computer and Data Security

- **FERPA** – *Family Educational Rights and Privacy Act* – Student data
- **HIPAA** – *Health Insurance Portability and Accountability Act* - Health information
- **GLBA** – *The Gramm-Leach-Bliley Act* – Nonpublic data
- **RFR** – *Red Flags Rule* – Identity theft prevention
- **PCI DSS** – *Payment Card Industry Data Security Standards* – Credit card information
Teachers and Administrators - Responsibility for securing data

*Show of Hands* – who is responsible?

A. 90% of security safeguards are technical and 10% rely on YOU, the computer user
B. 50% of security safeguards are technical and 50% rely on YOU, the computer user
C. 25% of security safeguards are technical and 75% rely on YOU, the computer user
D. 10% of security safeguards are technical and 90% rely on You, the computer user
Teachers and Administrators - Sensitive and Regulated Data

What is it? - Data that is protected against unwarranted disclosure through the establishment and practice of regulations and policies. Examples:

- **Personal Information:** SSN, human resource information, health information, educational records

- **Financial Information:** credit card numbers, loan information, bank account information
**SCENARIO:** You are a teacher and receive an e-mail by mistake. Included in the email is an excel file containing student names, addresses, social security numbers, etc.

**Show of Hands: What should you do?**

A. Immediately delete the e-mail and empty the deleted items
B. Notify the sender & your administrative office/data security dept.
C. Both A and B
D. Save the file to your computer
E. Ask your coworkers to review the file
F. Ignore it, and hope it mysteriously goes away
The correct answer is “C” - Immediately delete the e-mail, empty the deleted items folder, and notify the sender and your administration/information security department.

- This data could be FERPA, GLBA and RFR-protected data
- Never save or read e-mails when you are not the intended recipient
- Never save attachments from emails of which you were not the intended recipient…especially those including sensitive data
Computer and Data Security

Today’s Topics

• Why we need to know about data security
• Teachers and administrators and data security
• Safe computing practices for everyone
• Resources
Everyone - Safe Computing Practices
Secure Equipment and Data

- Lock down laptops and workstations
Everyone - Safe Computing Practices
Secure Equipment and Data

- Close down your browsers
- Enable password protected screen saver
- Do not leave sensitive papers or data on printers/fax machines
- Turn off computer at day’s end
- Lock your door
Everyone - Safe Computing Practices

Settings and Software

• Enable the computer’s firewall

Turn Windows Firewall on or off

1. Open Windows Firewall by clicking the **Start** button and then clicking **Control Panel**. In the search box, type **firewall** and then click **Windows Firewall**.

2. In the left pane, click **Turn Windows Firewall on or off**. If you’re prompted for an administrator password or confirmation, type the password or provide confirmation.

3. Click **Turn on Windows Firewall** under each network location that you want to help protect, and then click **OK**.

4. If you want the firewall to prevent all programs from communicating, including programs that you have previously allowed to communicate through the firewall, select the **Block all incoming connections**, including those in the list of allowed programs check box.

If you need to turn off Windows Firewall

**Warning**

- You should not turn off Windows Firewall unless you have another firewall enabled. Turning off Windows Firewall might make your computer (and your network; if you have one) more vulnerable to damage from worms or hackers.

Everyone - Safe Computing Practices
Settings and Software, con’t.

• Disable automatic logins
  (browser settings – Privacy & Security or Advanced Settings)

• Do not install or open unknown programs or files

• Password-protect your screen saver and set it to start after five minutes of inactivity
  (Control Panel > Power Options)

• Enable blocking of pop ups
  (browser settings – Privacy & Security or Advanced Settings)

• Control access to folders and file-shares
Everyone - Safe Computing Practices
Settings and Software, con’t.

• Turn on automatic updates/check frequently for software updates
  (Control Panel > System and Security > Windows Update)
• Check that your browser is up-to-date
• Review your application software
  (Control Panel > Programs > Programs and Features)
Everyone - Safe Computing Practices

Antivirus

- Ensure antivirus is installed and running
- Ensure antivirus definitions are current
- Turn on auto-scanning and real-time protection
- Use free antivirus scanning software
  - Malwarebytes - [https://www.malwarebytes.com/](https://www.malwarebytes.com/)
- Scan all removable media and email attachments
Everyone - Safe Computing Practices

Passwords

Show of Hands - Which is the better password?

A. LCP$@!%^*
B. !9*A7b$%b8%s
C. 2017AGGLESno1
D. Ilovetoplaybasketball
E. AdminAdmin
Everyone - Safe Computing Practices

Passwords

Construct strong passwords with:
• A password containing more characters; it’s more secure
• At minimum, set password to 8 characters with a combination of upper and lower case letters, numbers, and special characters

Protect your password
• Do not share your password with others
• Do not write down or post your password
• Do not use the same password for multiple purposes/accounts!
Everyone - Safe Computing Practices

Passwords

When possible, use a longer, easy-to-remember passphrase instead of a password. Example:

- Mydogatemyhomework!
- NewMexicoismyfavoritestate.
- Applepieandicecreamfordessert.
- Mygirlfriendstompedallovermyheart
Everyone - Safe Computing Practices
Protect Your Personal Data

Google yourself → Chris Lascano
Everyone - Safe Computing Practices
Protect Your Personal Data

Google yourself  

Chris Lascano

| 31. Christopher J Lascano | 29 | La Mesa, NM  
Mesquite, NM  
Las Cruces, NM | Ernest Lascano  
Susie Lascano |
Everyone - Safe Computing Practices
Protect Your Personal Data

Google yourself → Chris Lascano

<table>
<thead>
<tr>
<th>PERSON</th>
<th>AGE</th>
<th>LOCATIONS</th>
<th>RELATIVES</th>
</tr>
</thead>
<tbody>
<tr>
<td>Christopher J Lascano</td>
<td>29</td>
<td>La Mesa, NM</td>
<td>Ernest Lascano</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Mesquite, NM</td>
<td>Susie Lascano</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Las Cruces, NM</td>
<td></td>
</tr>
</tbody>
</table>

SEE RESULTS NOW >
Everyone - Safe Computing Practices
Protect Your Personal Data

Chris Lascano

Christopher J Lascano
Age: 25-29

Phone number
575-233-2124
CenturyLink Landline

Address
PO Box 987
Mesquite, NM 88048-0987

YIKES!
Everyone - Safe Computing Practices
Protect Your Personal Data

Other great sites to help gauge what’s out there:

- haveibeenpwnd.com – Shows sites were your account has been compromised
- pipl.com – Shows what is available on the web about you
- stalkscan.com – Show what information you are giving the world from your Facebook account
Phishing

Phishing attacks are designed to steal a person’s login and password information in order to take control of a victim’s account…

…and they…

…come to you as links in emails, tweets, posts, and online advertising.
Phishing emails have become harder to detect due to the cleverness of attackers and they appear as legitimate email. As you check your email, follow these practices:

- When in doubt, throw it out!
- If you didn’t expect it, reject it!
- Never enter your credentials from links provided by e-mail
- If unsure of the legitimacy of an e-mail, contact the sender
Everyone - Safe Computing Practices

Protect Your Personal Data

---

Phishing email example

---

We’re sorry to say goodbye

Hello,

iTunes let us know that you asked to cancel your membership. We’ve cancelled your membership effective Tuesday, March 21st, 2017.

Obviously we’d love to have you back. If you change your mind, simply restart your membership to enjoy all the best TV shows & movies without interruption.

RESTART MEMBERSHIP

We’re here to help if you need it. Visit the Help Center for more info or contact us.

–Your friends at Netflix
Everyone - Safe Computing Practices
Protect Your Personal Data

Hi <customer>,

This is a follow-up regarding your package delivery:

- Tracking Number: Op2uYq5R1ho

The package contained in the above-mentioned shipment was not accepted at the destination address. Please contact your local UPS office and provide the printed delivery sticker, included in this email.

Please note that in case of a failure to contact your local UPS office within 21 days the parcel will be returned to sender.

Thanks so much for shipping with UPS.
Because of unusual number of invalid login attempts on your account, we had to believe that, there might be some security problem on your account.

So we have decided to put an extra verification process to ensure your identity and your account security.

Please click on continue to the verification process and ensure your account security. It is all about your security.

Confirm that you're the owner of the account, and then follow the instructions.

Confirm all information, and then access your account as normal.

Thank you.

IMPORTANT INFORMATION
(If you cannot click on the link, please move the message into the Inbox).

Terms of use | Security | Privacy
From: Yohannes Bekele <ybekele@PSAV.COM>
Date: February 3, 2016 at 9:31:09 AM EST
To: Undisclosed recipients;
Subject: !!

You won $1M contact; pchlotto@pch-service.net

Confidentiality Notice: New Mexico has a very broad public records law. Most written communication to or from state employees are public records. Your email communications may therefore be subject to public disclosure. This email, including all attachments is for the sole use of the intended recipients. Any unauthorized review, use, disclosure or distribution is prohibited unless specifically provided under the New Mexico Inspection of Public Records Act.
Sir/Madam,

Our records indicate that you are a non-resident, and that you are exempted from the United States of America Tax reporting and withholdings on interest paid to you on your account and other financial benefits. To protect your exemption from tax and other financial benefits, you need to re-certify your exempt status to enable us confirm your records with us.

Therefore, you are required to authenticate the following by completing form W-8BEN attached and return same to us as soon as possible with a valid copy of government issued identifications (eg. International Passport) through fax number or the email at the bottom of the form.

List of required documents:
1. A copy of filled W-8BEN FORM.
2. A photocopy of the photo page of your international passport.

We appreciate your co-operation in helping us protect your exempt status and also confirm records.

Sincerely,

Mark Schneider,
IRS Public Relations
Everyone - Safe Computing Practices
Protect Your Personal Data

This email address does not match. This email was sent to a few of my contacts in my Yahoo email.

Phishing email example
Everyone - Safe Computing Practices
Protect Your Personal Data

Phishing email example
Although the above website may look familiar or legitimate, take a close look at the web address. Notice it’s not from NMSU, but from an external source, “justhost.com”.

Protect Your Personal Data

Phishing - Spotting a bad URL

Everyone - Safe Computing Practices

Office 365 Portal

Enter your myNMSU username and password.

Username: 
Password: 

Sign In
Everyone - Safe Computing Practices
Protect Your Personal Data

Phishing - Spotting a good URL
Make a copy

• Frequency and method of backup depends on the data's value
• Backup to:
  • Institution’s backup facility
  • Using existing MS Office System Software
  • Free cloud services, see: https://www.thebalance.com/free-cloud-storage-1356638
  • Portable device: external hard drive or USB/flash drive
  
Remember to lock this up. Recommendation: a water/fire proof safe
Everyone - Safe Computing Practices
Protect Your Personal Data

Make a copy
• To portable device (1 TB)
  range $54 - $1,500

https://www.amazon.com/Elements-Portable-External-Drive-WDBUZG0010BBK-WESN/dp/B00CRZ2PRM/ref=sr_1_2?ie=UTF8&qid=1509904115&sr=8-2&keywords=external+drive
Everyone - Safe Computing Practices

Safe Network Practices

- Set a password to access your home router
- Change home router admin account name and password
- Use encrypted wireless networks when transmitting private data, such as NMSU’s Aggie Air, WPA2
- Use VPN – Virtual Private Networks when possible
Everyone - Safe Computing Practices
Safe Network Practices

DO NOT use these wireless connections for anything “IMPORTANT!”
Don’t:
• Save sensitive data on your computer unless necessary
• Gossip or share sensitive data with others
• Look up confidential data for co-workers or students who do not have access without your supervisor’s approval
• Throw reports or printouts that have sensitive data in the trash
Everyone - Safe Computing Practices
General Safe Practices

Don’t:
• Install a network printer in your office without consulting your computer support technician
• Install a wireless access point without consulting your computer support technician
• Use found USBs/flash drives
Everyone - Safe Computing Practices
General Safe Practices

Do:

• Use encryption for sensitive data
  For example, add a password to your Word Document (steps for PPT and Excel).
    File > Info > Protect Document > Encrypt with Password

• Check new documents for hidden properties or personal information
  Steps below for Word, PPT, and Excel
    File > Info > Check for Issues > Inspect Document
Computer and Data Security

Today’s Topics

• Why we need to know about data security
• Teachers and administrators and data security
• Safe computing practices for everyone
• Resources
Resources
Government Accounts and Credit Monitoring

• Freezing your credit: https://www.consumer.ftc.gov/articles/0497-credit-freeze-faqs
• Establish accounts at ssa.gov and irs.gov
• Consumer reports advice: https://www.consumerreports.org/equifax/how-to-lock-down-your-money-after-the-equifax-breach/
Resources
Child Safety

• **Keeping Children Safe,**

• **Keeping Your Child Safe on the Internet,**

• **Protecting Kids Online,**
  FTC: https://www.consumer.ftc.gov/topics/protecting-kids-online
Resources Hacked?

- *I’ve Been Hacked, Now What?*  
  Livewire: [https://www.lifewire.com/ive-been-hacked-now-what-2487230](https://www.lifewire.com/ive-been-hacked-now-what-2487230)


- *How to Check If Your Accounts Have Been Hacked*, Techlicious: [https://www.techlicious.com/tip/how-to-check-if-your-password-has-been-stolen/](https://www.techlicious.com/tip/how-to-check-if-your-password-has-been-stolen/)
Resources
Security Tips


- **General Tips & Advice**, STOP. THINK. CONNECT: https://stopthinkconnect.org/tips-advice/general-tips-and-advice

- **A Teacher’s Guide to Student Online Safety**, Stay Safe Online: https://staysafeonline.org/blog/teachers-guide-student-online-safety/
National Cyber Security Awareness Month (NCSAM)

• Every October #CyberAware
• Get involved - https://staysafeonline.org/ncsam/get-involved/
• Have a bulletin board? Take a poster!

Coming January 28, 2018

Data Privacy Day
Data Privacy Day is an international effort to empower individuals and encourage businesses to respect privacy, safeguard data and enable trust.

#PrivacyAware
Keeping Your Data Safe

Questions?

John Roberts
Director of Computer Systems and
Chief Information Security Officer

Presentation: infosec.nmsu.edu