Computer and Data Security

John Roberts
NMSU Director of Computer Systems and Chief Information Security Officer

Security is everyone’s responsibility!
Computer and Data Security

Today’s Topics

• Why we need security training
• Security Policies
• Data security
• Safe computing practices and scenarios
• Resources
Computer and Data Security

Today’s Topics

• Why we need security training
• Security Policies
• Data security
• Safe computing practices and scenarios
• Resources
Why we need security training

- To help us better understand how to protect NMSU data resources from malicious attacks
- To comply with legal and regulatory requirements
Computer and Data Security

Today’s Topics

• Why we need security training
• **Security Policies**
• Data security
• Safe computing practices and scenarios
• Resources
Regulatory Requirements - Computer and Data Security

- **FERPA** – *Family Educational Rights and Privacy Act* – Requirement for the protection of the privacy of student data
- **HIPAA** – *Health Insurance Portability and Accountability Act* – Requirement for the protection of health information
- **GLBA** – *The Gramm-Leach-Bliley Act* – Requirement for the protection of nonpublic data
- **RFR** – *Red Flags Rule* – Requirement for Identity theft prevention
- **FISMA** – *Federal Information Security Management Act* – Requirement for the proper protection and security of Federal data
- **PCI DSS** – *Payment Card Industry Data Security Standards* – Requirement for the protection of credit card information
Risks of Non-Compliance

NMSU student and employee data could be lost or exposed, leading to:

• Damage to NMSU’s reputation and subsequent loss of public trust
• Fines
• Identity theft and privacy violations
• Loss of the ability to do business
Computer and Data Security

Today’s Topics

• Why we need security training
• Security Policies
• Data security
• Safe computing practices and scenarios
• Resources
Data security – What is it?

Data security is the practice of keeping data protected from unauthorized access and corruption or loss.
Responsibility for securing NMSU 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
Sensitive and regulated data

What is it? - Data that is protected against unwarranted disclosure through the establishment and practice of regulations and policies is considered sensitive and regulated data.

Examples:

• **Personal Information:** Social Security Numbers, Human Resource Information, Health Information, Educational Records
• **Financial Information:** Credit Card Numbers, Loan Information, Bank Account Information
• **Private Research Data** or any other information that is not intended to be made available to the public.
Show of Hands – what in the list below is considered sensitive and regulated data?

A. Student Name
B. Student Name with grade
C. Customer credit card data
D. Employee Name
E. Employee Name with medical data
F. Aggie ID/Banner number
The correct answers are “B, C, and E” - Most of the time data without an identifying element is not sensitive. However, combining multiple data types can create sensitive data

- B is FERPA data because the name of a student is associated with their grade.
- C is PCI/DSS data, any credit card data is protected by this agreement
- E is HIPAA data because medical information is associated with Employee

A, D, and F are data elements that, on their own, do not provide identity. In fact all of these items are publicly available.
SCENARIO: You are an NMSU employee and receive an e-mail by mistake. Included in the email is an excel file containing 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 and the Information Security department
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 and empty the deleted items and notify the sender and the Information Security department (infosec@nmsu.edu).

• This type of data may fall under various regulatory requirements including FERPA, GLBA and RFR, which protects the privacy of sensitive data.
• You should never save or read e-mails when you are not the intended recipient. Additionally, you should not save unintended attachments especially those including sensitive data.
Computer and Data Security

Today’s Topics

• Why we need security training
• Security Policies
• Data security
• **Safe computing practices and scenarios**
• Resources
Safe computing practices and scenarios

- Secure your area
- Secure your computer
- Keep software up-to-date
- Set strong passwords
- Protect your computer from viruses and hacking
- Protect your personal data
- Identify phishing attacks
- Backup your NMSU data
- Using NMSU Wireless/VPN
- Dos and Don’ts of data security
Safe computing practices - Secure your area

- Secure equipment and data before leaving an area unattended
- Physically lock down laptops and workstations when possible or close your office door if possible
- Close down your browser after visiting a web site with sensitive data
- Enable password protected screen saver and log off when you step away
- Do not leave sensitive papers or data on printers or fax machines
Safe computing practices - Secure your computer

- Enable the computer’s firewall before you connect to the internet
- Disable automatic login and guest accounts
- Do not install or open unknown programs or files
- Control access to folders and file-shares
- Shut-off your computer at the end of your work day
Safe computing practices - Secure your computer, cont.

- Ensure your computer is enrolled in your department’s domain
- Install an anti-virus and run regular scans
- Disable automatic login and guest accounts
- Do not install or open unknown programs or files
- Password-protect your screen saver and set it to start after five minutes of inactivity
Safe computing practices -
Keep software up-to-date

- Turn on automatic updates
- Check frequently for updates
- Check your browser
- Check your application software
- Ensure antivirus client and definitions are current
Safe computing practices - Set strong passwords

Show of Hands - Which is the better password?

A. NMSU@!%$^  
B. !9*A7b$%b8%s  
C. 2017AGGIESno1  
D. Ilovetoplaybasketball  
E. AdminAdmin
Safe computing practices -
Set strong passwords

Construct strong passwords with:
• A password with more characters is more secure
• NMSU accepts passwords up to 16 characters
• A minimum of 8 characters and 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
Safe computing practices - Set strong passwords

• Use a passphrase instead of a password, for example:
  • Mydogatemyhomework!
  • NewMexicoismyfavoritestate.
  • Applepieandicecreamfordessert
  • Mygirlfriendstompedallovermyheart
Single Log-in vs. Single Sign-on

- NMSU previously instituted single login. Meaning, using your NMSU username/password to login to most NMSU systems you visit online.
- Now, moving toward single sign-on for all NMSU applications online. Sign-in once with your NMSU username/password and browse through various applications after logging in once.
  - Goal - You will see the same login page for all applications.
- To single log-off, close your browsers.
Safe computing practices - Protection from viruses and hacking

- Use anti-virus software
  - Get free anti-virus: http://help.nmsu.edu/security-anti-virus/#Sophos
  - *Note: NMSU will be upgrading Sophos Soon!*

- Ensure your virus definitions are current

- Turn on auto-scanning and real-time protection

- Scan all removable media and email attachments
Safe computing practices - Protect your personal data

Google yourself → Chris Lascano
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 |
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>Mesquite, NM, La Mesa, NM, Las Cruces, NM</td>
<td>Ernest Lascano, Katrina Lascano, Susie Lascano</td>
</tr>
</tbody>
</table>

SEE RESULTS NOW >
Safe computing practices - Protect your personal data

Know what’s out there!  

Chris Lascano

Christopher J Lascano
Age: 25-29

Phone number
575-233-2124
CenturyLink Landline

Address
PO Box 987
Mesquite, NM 88048-0987

YIKES!
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
Safe computing practices -
Identify “Phishing” attacks

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.
Safe computing practices - Identify “Phishing” attacks

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, always forward it to abuse@nmsu.edu
Safe computing practices - Identify “Phishing” attacks

From: Anderle, Gary [mailto:Gary.Anderle@Mercy.Net]
Sent: Monday, February 15, 2016 10:25 AM
To: info@ghfftg.net
Subject: Notification: IT Support Center

IT systems is currently migrating all email accounts to Outlook Web access 2016. In order to keep your account and information, you must activate your account 48 hours of receiving this email or your account will be disabled: Click on the link below and fill required information to keep your account running.

ACTIVATE HERE

All email will be re-activated. Your account will not function if you do not upgrade.
Global IT Support Center

This electronic mail and any attached documents are intended solely for the named addressee(s) and contain confidential information. If you are not an addressee, or responsible and delivering this email to an addressee, you have received this email in error and are notified that reading, copying, or disclosing this email is prohibited. If you received this email in error, immediately reply to the sender and delete the message completely from your computer system.
Safe computing practices - Identify “Phishing” attacks

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.

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
Safe computing practices - Identify “Phishing” attacks
Safe computing practices - Identify “Phishing” attacks

SCENARIO: While checking your email, you see a message stating that you have run out of data space on your email acct. The email contains a “Click Here” link to sign into your account. You click the link and see the following:

Show of Hands: Do you enter your credentials? YES or NO?
Safe computing practices - Identify “Phishing” attacks

Correct answer: NO WAY, JOSE!

Never provide your credentials from e-mail requests! NMSU ICT will never ask for your password!
Safe computing practices - Identify “Phishing” attacks

Correct answer: NO WAY, JOSE!

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”.
Safe computing practices - Backup your NMSU data

• Backup important NMSU data to removable media or an appropriate backup service
  • ICT offers a backup service for a small fee. Call 646-1840 for more information
  • Frequency and method of backup depends on the data's value
• Secure backup media to protect sensitive data.
• Delete unneeded files according to NMSU’s Record Retention Administrative Rule.
Safe computing practices - Using NMSU wireless/VPN

• For official NMSU Business only use **AggieAir-WPA2** wireless
  • NMSU wireless networks, AggieAir and AggieGuest, as well as other publicly accessible wireless networks, are not secure because traffic is not encrypted and should only be used with the NMSU VPN.

• NMSU VPN – Virtual Private Network
  • Provides a secure encrypted connection from your computer only to the NMSU network.
  • NMSU computer users can start using the VPN by going to https://vpn.nmsu.edu
  • All employees accessing NMSU data remotely should use the VPN
  • Access to Banner and Cognos from off campus requires the VPN
Safe computing practices - Using NMSU wireless/VPN

NMSU Wireless. (AggieAir or AggieGuest) is convenient, but not secure because traffic is not encrypted. Hackers can view data as it goes to the internet.

DO NOT use these wireless connections for anything “IMPORTANT”!
Safe Computing practices - Dos and Don’ts of security

• Don’t save sensitive data locally to your computer unless absolutely necessary
• If there is a business reason to store sensitive data on your computer, it should be encrypted
  • *All NMSU devices need to be encrypted*
• Don’t gossip or share sensitive data with others
• Don’t look up confidential data for co-workers or student who do not have access without your supervisor’s approval
• Don’t throw reports or printouts that have sensitive data in the trash without shredding them first
• Don’t install a network printer in your office without consulting your computer support technician
• Don’t install a wireless access point without consulting your computer support technician
Safe Computing practices - Dos and Don’ts of security

SCENARIO: You have received a phone call from someone that identifies herself as a vendor for your manager. She asks you to verify the account number and appropriate approver’s name.

*Show of Hands:* Should you share this information? (Yes or No)
Safe Computing practices - Dos and Don’ts of security

SCENARIO: You have received a phone call from someone that identifies herself as a vendor for your manager. She asks you to verify the account number and appropriate approver’s name.

The correct answer is “No”

When in doubt, DO NOT share sensitive information. Ask the individual for contact information and provide it to your manager. Data-privacy regulations prohibit the improper disclosure of sensitive information and may subject NMSU to regulatory fines.
Safe Computing practices - Dos and Don’ts of security

Report incidents that involve:

• *University data/confidential information* – should be reported immediately to the IT Compliance Officer at 646-5902 or itcompliance@nmsu.edu

• *General computing issues such as e-mail phishing attacks, viruses, etc.* – should be reported to the Chief Information Security Officer at 646-7992 or ciso@nmsu.edu

*When in doubt, report to both officers*
Safe Computing practices - Dos and Don’ts of security

SCENARIO: Your car has been broken into and all of your bags are missing. You don’t touch anything and call the police and your insurance company. You realize that one of the bags contained an NMSU laptop and it may contain confidential data.

Show of Hands: What should you do?

A. Contact your supervisor and get it replaced and don’t worry about the data that was on the laptop
B. Report the incident to Legal Counsel
C. Report the incident to your supervisor and the IT Compliance Officer or Chief Information Security Officer (CISO)
D. Purchase an identical computer using your own personal funds
Safe Computing practices - Dos and Don’ts of security

The correct answer is “C” – Report the incident to your supervisor and the IT Compliance Officer or the Chief Information Security Officer (CISO).

The IT Compliance Officer and CISO can properly handle the incident and will report it to the appropriate federal agency.
Safe Computing practices - Dos and Don’ts of security

SCENARIO: Sara is an employee at NMSU who handles wire transfers and other payments in her normal work day. Sara, who doesn’t normally receive emails from the president, received the email below:

From: Garrey Carruthers <Garrey@nmsu.edu>
Sent: Wednesday, August 3, 2016 8:38 AM
To: [REDACTED]@ad.nmsu.edu
Subject: wire transfer

Dear Sara,

I need you to process a wire transfer payment for service rendered. What details will be needed to process the payment?

Garrey Carruthers
Safe Computing practices - Dos and Don’ts of security

SCENARIO: Sara is an employee at NMSU who handles wire transfers and other payments in her normal work day. Sara, who doesn’t normally receive emails from the president…

Show of Hands: What should Sara do?

A. Reply to the email with the information needed to make a transfer payment
B. Report the email to the Information Security Department to check the legitimacy of the email
C. Reply to the email and try to verify if it is in fact the President on her own
D. Call her friends and tell them that she and the prez are BFFs
SCENARIO: Sara is an employee at NMSU who handles wire transfers and other payments in her normal work day. Sara, who doesn’t normally receive emails from the president…

The correct answer is “B”

Report the email to ICT’s Information Security Department to check the legitimacy of the email. It is very easy for hackers to fake or impersonate email addresses. If you receive similar questionable or suspicious emails please report them to the Information Security Department by forwarding them to abuse@nmsu.edu.

For more information please visit infosec.nmsu.edu.
Computer and Data Security

Today’s Topics

• Why we need security training
• Security Policies
• Data security
• Safe computing practices and scenarios
• Resources
Resources - Sophos Upgrade

Students

- Endpoint Protection

Staff (Cloud based second gen capabilities)

- Central Endpoint Advanced
- Central Endpoint Intercept X
Resources - Multifactor Authentication

• ICT has purchased a DUO license for students and Staff

• Piloting multiple small deployments: Privileged account access for application and OS administrators.

• Plan to deploy in front of NMSU portal

• Plan to deploy for NMSU VPN Access
Resources - Equifax data breach

- Freeze your credit
- Establish accounts at ssa.gov and irs.gov
- Credit Monitoring

https://www.consumerreports.org/equifax/how-to-lock-down-your-money-after-the-equifax-breach/
For more information, visit:

**NMSU IT Compliance**

http://itcompliance.nmsu.edu/
Telephone 646-5902
E-mail itcompliance@nmsu.edu

**NMSU Information Security**

http://infosec.nmsu.edu/
Telephone 646-7992
E-mail sysjcr@nmsu.edu
Computer and Data Security

John Roberts
NMSU Director of Computer Systems and Chief Information Security Officer

Questions?
IT Meeting

• Security Concerns
• Scanning
• Network Visibility
• Any Other Topics