Security Awareness

Rick Whitmore

Information Technology
Security Office
security.ku.edu
“Everyone has a role in securing their part of cyberspace, including the devices and networks they use.”
Today’s Topics

• Impact on Universities
• KU Policy
• Passwords
• Social Engineering
• Mobile Devices, Travel
RISKS?

- Financial Damage
- Reputation Damage
- Loss of Customers
- Loss of Grant Funding
- Fines (civil and criminal)
- Prison

HIPAA – Fines and Prison
FERPA – Cutoff of Federal Funding
Gramm-Leach Bliley – Fines and Prison
PCI – Civil fines starting at $50,000
CUI - Controlled Unclassified Information
NIST 800-171
March 17, 2014

Data Breaches Put a Dent in Colleges’ Finances as Well as Reputations

- University of Maryland
  - 309,079 student and personnel records, dating to 1998
- Indiana University
  - information on 146,000 students exposed for 11 months.
- North Dakota University system
  - 291,465 former, current, and aspiring students and 784 employees

“The average per-record cost across industries including government, health care, and retail is $136”
Data breach could cost $3 million, Michigan State says

“Names and MSU identification numbers were exposed along with social security numbers, which are extremely valuable to criminals . . .”

“. . . a data breach that affected about 400,000 records and included names, Social Security numbers and MSU identification numbers . . .”
…federal regulators have slapped the University of Massachusetts Amherst with a $650,000 financial settlement and corrective action plan after investigating a relatively small 2013 breach involving a malware infection at a campus speech and language center.”

“An intensive evaluation of the incident located no evidence suggesting or indicating that any data was copied from the workstation, but could not rule out the possibility.”
“Russian-Speaking Hacker Sells Unauthorized Access to Over 60 Universities and Government Agencies”

U.S. University Victims

- Cornell University
- Virginia Tech
- University of Maryland, Baltimore County
- University of Pittsburgh
- New York University
- Rice University
- University of California, Los Angeles
- Eden Theological Seminary
- Arizona State University
- NC State University
- Purdue University
- Atlantic Cape Community College
- University of the Cumberlands
- Oregon College of Oriental Medicine
- University of Delhi
- Humboldt State University
- The University of North Carolina at Greensboro
- University of Mount Olive
- Michigan State University
- Rochester Institute of Technology
- University of Tennessee
- St. Cloud State University
- University of Arizona
- University at Buffalo
- University of Washington
October 5, 2010

Chapel Hill Researcher Fights Demotion After Security Breach
Laptops Lost Like Hot Cakes at US Airports

By Agam Shah
IDG News Service | JUN 30, 2008 12:30 PM PT

University of Oklahoma
- July 2015
  - Stolen unencrypted laptop from car
  - 7,700 records
  - patients’ names, dates of birth, medical procedure dates, medications, lab results, admission and discharge dates, treating physicians’ names, and treatment plans.

- October 2015
  - Stolen unencrypted laptop from car
  - 9,300 records
  - patients’ first and last names, medical record numbers, and dates of birth, and in some cases, patients’ age, physicians’ names, and diagnosis, treatment, and/or billing codes

Stolen Laptop Leads to Possible Healthcare Data Breach in KS

Recent healthcare data breaches include cases of unencrypted email and a stolen hard drive.

Security Office offers whole disk encryption service, contact your support staff
KS Breach Notification Law

- "Security breach" means the unauthorized access and acquisition of unencrypted or unredacted computerized data that compromises the security, confidentiality or integrity of personal information maintained by an individual or a commercial entity and that causes, or such individual or entity reasonably believes has caused or will cause, identity theft to any consumer.

Article 7a. - PROTECTION OF CONSUMER INFORMATION
KU Policy Library

Contains all policies relevant to your presence at KU

http://policy.ku.edu/
Data Classification

- **Level I – Confidential Information:** High risk of significant financial loss, legal liability, public distrust, or harm if this data is disclosed. [Examples](#)

- **Level II – Sensitive Information:** Moderate requirement for Confidentiality and/or moderate or limited risk of financial loss, legal liability, public distrust, or harm if this data is disclosed. [Examples](#)

- **Level III – Public Information:** Low requirement for Confidentiality [information is public] and/or low or insignificant risk of financial loss, legal liability, public distrust, or harm if this data is disclosed. [Examples](#)
Level 1 Examples

- Data protected by HIPAA (health information)
- Data protected by FERPA
  - (student information including grades, exams, rosters, official correspondence, financial aid, scholarship records, etc.)
- Personally Identifiable Information (“PII”)
- Individually identifiable information created and collected by research projects
- Data subject to other Federal or state confidentiality laws
- Personnel data
KU Resources

• Research file storage
  – Greg Smith
  – http://tsc.ku.edu/research-team
  – itrs@ku.edu

• Research Data Management
  – http://guides.lib.ku.edu/data
  – Jamene Brooks-Kieffer
    Data Services Librarian
    Phone: (785) 864-5238
    Email: jamenebk@ku.edu
Cloud Data Breaches in last 3 years

- Dropbox – 69 million
- Myspace – 360 million
- Tumblr – 73 million
- Twitter – 43 million
- Yahoo – 500 million

Plus dozens of adult, adult-dating etc. sites
LinkedIn data breach blamed for multiple secondary compromises

- 4988 KU email addresses
- cracked 2120 passwords of 3443, 62%
  - password: 10
  - rockchalk: 10
  - kansas: 11
  - jayhawk: 29
- 769 active KU accounts
- 4 accounts using current KU credentials

- Academic Advisor
- Academic Affairs Coordinator
- Accounting Specialist
- Accompanist
- Assistant Coach
- Assistant Dean
- Assistant Vice Provost
- Associate Dean
- Associate Director
- Associate Professor
- Associate Vice Provost
- Communications Coordinator
- Dean
- Development Coordinator
- Development Director
- Director of Marketing
- Executive Associate
- Grant Coordinator
- IT Analyst
- IT Technology Coordinator
- Lecturer
- Library Assistant
- Library Associate
- Media Coordinator
- Office Manager
- Professor
- Professor Emeritus
- Program Coordinator
- Research Professor
- Research Project Director
- Vice Provost
Choosing Passwords

1. Memorable phrase, “I like ham and cheese sandwiches”.
2. Remove spaces, “ilikehamandcheesesandwiches”
3. Use shorthand, and misspell words, “ilykhamandchzsammies”
4. Use some characters, numbers and mix case
   
   1IYkh4m&chZsa2mies

It would take a desktop PC about 71 quadrillion years to crack this password

https://howsecureismypassword.net/
28 bits of entropy: 3 days at 1000 guesses/sec

Difficulty to guess: EASY

Difficulty to remember: HARD

44 bits of entropy: 550 years at 1000 guesses/sec

Difficulty to guess: HARD

Difficulty to remember: You’ve already memorized it

Through 20 years of effort, we’ve successfully trained everyone to use passwords that are hard for humans to remember, but easy for computers to guess.
Password Managers

Web-Based
- Need STRONG master password
- Subject to cloud security problems

Desktop
- Need STRONG master password
- Cross Platform
- Mobile versions
- Less accessible/Convenient
Two-step Authentication

- A thing you know
  - Username, password
- A thing you have
  - Token
  - Code sent to phone or other device

Google Authenticator

Setup Two-Factor Authentication

- Services
  - Google
  - Facebook
  - Dropbox
  - LastPass
  - Twitter
  - Amazon
“Without staff awareness of social engineering scams and techniques, con artists will find the college and university environment an easy target.”

http://www.securityweek.com/higher-education-perfect-security-storm
A serious malfunction has been detected with OS X 10.11 and your Firefox 47.0.

Please call the toll-free number below for a Microsoft-Certified Technician to help you resolve the issue:
1-855-998-8206

For your safety, closing the Firefox browser has been disabled without support of the Apple Macintosh technician to avoid corruption to the registry of your OS X 10.11 operating system.

Do not shut down or restart the computer doing that may lead to data loss and possible failure of the operating system and potential non-bootable situation resulting in complete data loss. Please contact Microsoft-Certified Technician at the toll-free keypad 1-855-998-8206

DO NOT RESTART COMPUTER AS IT MAY CAUSE PERMANENT HARD DRIVE FAILURE
CALL MICROSOFT-CERTIFIED TECHNICIAN TOLL FREE 1-855-998-8206
Don’t Ignore Web Warnings!

This Connection is Untrusted

You have asked Firefox to connect securely to [redacted], but we can’t confirm that your connection is secure.

Normally, when you try to connect securely, sites will present trusted identification to prove that you are going to the right place. However, this site’s identity can’t be verified.

What Should I Do?

If you usually connect to this site without problems, this error could mean that someone is trying to impersonate the site, and you shouldn’t continue.

- Get me out of here!
- Technical Details
- I Understand the Risks
Dear KU-Web Subscriber,

We are currently carrying out maintenance and upgrade of our KU Web-mail service and as a result of this; our E-mail client has been changed and your original password will be reset. Please provide us your User name: (******) Password(******) for reactivation.

Thanks for using KU University's Web services

Information Technology
1001 Sunnyside Ave.
Lawrence KS 66045
(785) 864-8080
We Phished You!

- October 3, 2016
- All faculty and staff were sent message (11,846)
- 743 credentials submitted
- Top titles
  1. GTA
  2. GRA
  3. Professor
  4. Retired Staff
  5. Lecturer

Most submitted credentials were from off-campus
“Success Rates”
- Faculty: 10%
- GA: 27%
- GTA: 16%
- GRA: 18%
- Student Staff: 25%
- Unclassified: 8%
And one more

Parking Fine T6342910

Traffic Enforcement <meterreader@citytrafficpatrol.net>
Wednesday, April 26, 2017 at 4:32 AM
To: Kopsa, Teresa A

You get a parking fine!

29-938 - Failure to follow signs

Court appearance required

Parking ticket number information: T6342910

Parking Fine

To pay your parking fine, download your ticket and choose one of 3 convenient ways:

1. Online
   Pay online by Visa or Mastercard, $2 processing fee here

1. By Mail
   Pay by mail to the traffic dept.

Best regards,
Traffic Enforcement

If you consider that you have received a parking ticket in error, you can apply for rectification. You can do this by visiting the traffic enforcement in the community where you received the parking ticket. You must take your parking ticket with you. If your application is not approved, you can write and contest your liability to pay (appeal). Send your letter to the address stated on the parking ticket. Keep in mind that the parking fine must be paid even if you consider it to be in error. The fine will be refunded to you if your application is approved.
27% “success”
- 54% GTA/GRA
- 14% Unclassified Staff
- 49% Student Staff
- 16% Faculty
RE: ICT Scheduled maintenance update.

O Lisa Freeman <lisa.freeman@courts.nsw.gov.au>
Friday, July 1, 2016 at 7:52 AM
To: O Lisa Freeman

Impacted Groups: 2016 Outlook/Exchange Users

If you are receiving this message, the Outlook/Exchange email servers that provide your email service will undergo scheduled maintenance tonight, July 1, 2016 from 07:00pm to 2:00am.

Please click [here](#) and log in to your Outlook client prior before 07:00 PM today to enable auto backup of all information on your mailbox, if you do not log into the auto backup portal, you may lose the connection to your mailbox including all your information during the maintenance.

If you find it difficult to send or receive messages from your Outlook client after the maintenance period, or tomorrow morning, please close Outlook and then log in again.

We regret this inconvenience and appreciate your patience.

--------------------------------------------------------

PLEASE DO NOT REPLY DIRECTLY TO THIS MESSAGE.

This is a Broadcast e-mail sent on behalf of the Sender and/or Department. If you wish to respond, please follow the contact instructions in the message ONLY.
RE: ICT Scheduled maintenance update.

To: Lisa Freeman <lisa.freeman@courts.nsw.gov.au>

Friday, July 1, 2016 at 7:52 AM

Impacted Groups: 2016 Outlook/Exchange Users

If you are receiving this message, the Outlook / Exchange email servers that provide your email service will undergo scheduled maintenance tonight, July 1, 2016 from 07:00pm to 2:00am

Please Click here and log in to your Outlook client prior before 07:00 PM today to enable auto backup of all information's on your mailbox, if you do not log into the auto backup portal, you may lose the connection to your mailbox including all your information's during the maintenance.

If you find it difficult to send or receive messages from your Outlook client after the maintenance period, or tomorrow morning, please close Outlook and then log in again.

We regret this inconvenience and appreciate your patience.

__________________________________________
PLEASE DO NOT REPLY DIRECTLY TO THIS MESSAGE.

This is a Broadcast e-mail sent on behalf of the Sender and/or Department. If you wish to respond, please follow the contact instructions in the message ONLY.

FAKE!
From: Microsoft account team [mailto:account-security-noreply@account.microsoft.com]
Sent: Wednesday, June 22, 2016 7:19 AM
To: New, Judy Lynn <jnew@ku.edu>
Subject: Microsoft account security alert

Microsoft account

Security alert

We think that someone else might have accessed the Microsoft account jm****@ku.edu. When this happens, we require you to verify your identity with a security challenge and then change your password the next time you sign in.

If someone else has access to your account, they have your password and might be trying to access your personal information or send junk email.

If you haven't already recovered your account, we can help you do it now.

Recover account

Learn how to make your account more secure.

Thanks,
The Microsoft account team
From: Microsoft account team [mailto:account-security-noreply@account.microsoft.com]
Sent: Wednesday, June 22, 2016 7:19 AM
To: New, Judy Lynn <jnew@ku.edu>
Subject: Microsoft account security alert

Microsoft account

Security alert

We think that someone else might have accessed the Microsoft account jn****@ku.edu. When this happens, we require you to verify your identity with a security challenge and then change your password the next time you sign in.

If someone else has access to your account, they have your password and might be trying to access your personal information or send junk email.

If you haven't already recovered your account, we can help you do it now.

Recover account

Learn how to make your account more secure.

Thanks,
The Microsoft account team
Message from KU Payroll Department

To: Payroll Department <do_not_reply_emory_edu@oph-dazd.com>

Friday, June 10, 2016 at 8:31 AM

Your Pay Advice is now ready for online review on KU HR/Pay Employee Self-Service:

https://hrku.edu

If you have any questions, please contact your Payroll Department.

PLEASE DO NOT REPLY TO THIS MESSAGE. IT WAS SENT FROM AN AUTOMATED SYSTEM AND REPLIES WILL NOT BE ANSWERED.
Message from KU Payroll Department

Payroll Department <do_not_reply_emory_edu@oph-dazd.com>
Friday, June 11, 2010 at 8:31 AM
To:

Your Pay Advice is now ready for online review on KU HR/Pay Employee Self-Service:
https://hr.ku.edu

If you have any questions, please contact your Payroll Department.

PLEASE DO NOT REPLY TO THIS MESSAGE. IT WAS SENT FROM AN AUTOMATED SYSTEM AND REPLIES WILL NOT BE ANSWERED.

http://www.chaseny-inv.com/hr_ku_edu/psp/hrprd/index_cmd_loginlanguageCd_ENG.html

FAKE!
HR/Pay
KU Human Resources
KUMC Human Resources

Updates
Welcome to the University's Human Resource and Payroll System

Online Training
• HCM Navigation and Fundamentals
• Recruiting
• Absence Management, Time Reporting and Payroll
• Benefits

University of Kansas
785-864-8060 | HRsc@ku.edu
KU HR/Pay Resources

University of Kansas Medical Center
913-586-7995
KUMC HR/Pay Resources

Log in using your KU or KUMC Online ID and password

By clicking 'Sign in', you agree to conduct business electronically with the University of Kansas. In addition, you agree to use your authorized online account, and are solely responsible for all use of your account as of the date of this agreement. Your account will be subject to change and could be closed at any time, subject to our policies. You are responsible for maintaining the confidentiality of your account. You agree to promptly notify us of any unauthorized use or breach of security of your account.

I also agree to comply with the policies of the University of Kansas regarding the proper use of computing resources. Knowingly accessing, modifying, or altering confidential information, deleting files, or manipulating system or network functions or structure, is prohibited. This includes the right to impose disciplinary action up to and including dismissal. www.policy.ku.edu

Online ID:
Password:
Forgot your KU password? | Forgot your KUMC password?

Sign in
KU employees fall victim to phishing scam, lose paychecks

Phishing campaign targeted at faculty and staff thought to be highly compensated.
Spear- phish, with malicious attachment
-----Original Message-----
From: Yolanda Deibler [mailto:deibler.yolandajrix@outlook.com]
Sent: Sunday, December 04, 2016 8:52 AM
To: [Redacted] <curbas@ku.edu>
Subject: FWD cvrbas

Whats up

You will be charged $1,288.39 on your current Mastercard card soon.
View attachment to avoid it.
Pwd to open the doc is 7778.

Warmest regards
Rosa
CERBER RANSOMWARE

Your documents, photos, databases and other important files have been encrypted!

If you understand all importance of the situation then we propose to you to go directly to your personal page where you will receive the complete instructions and guarantees to restore your files.

There is a list of temporary addresses to go on your personal page below:

http://avsxrcq2q5fgrw2.zh5mu9.bid/1FE1-0C7C-FA14-005D-4F60
http://avsxrcq2q5fgrw2.x29u3l.top/1FE1-0C7C-FA14-005D-4F60
http://avsxrcq2q5fgrw2.onion.to/1FE1-0C7C-FA14-005D-4F60
http://avsxrcq2q5fgrw2.onion/1FE1-0C7C-FA14-005D-4F60 (TOR)

File open 8:40:22
Encryption starts 8:40:51
Full user profile encrypted 8:46:33
Can't you find the necessary files?
Is the content of your files not readable?

It is normal because the files' names and the data in your files have been encrypted by "Cerber Ransomware".

It means your files are NOT damaged! Your files are modified only. This modification is reversible.
From now it is not possible to use your files until they will be decrypted.

The only way to decrypt your files safely is to buy the special decryption software "Cerber Decryptor".

Any attempts to restore your files with the third-party software will be fatal for your files!

You can proceed with purchasing of the decryption software at your personal page:

http://avsxrcq2q5fgrw2.zh5mu9.bid/1FE1-0C7C-FA14-005D-4F60
http://avsxrcq2q5fgrw2.x29u3l.top/1FE1-0C7C-FA14-005D-4F60
http://avsxrcq2q5fgrw2.onion.to/1FE1-0C7C-FA14-005D-4F60

If this page cannot be opened click here to generate a new address to your personal page.

At this page you will receive the complete instructions how to buy the decryption software for restoring all your files.

Also at this page you will be able to restore any one file for free to be sure "Cerber Decryptor" will help you.
Your documents, photos, databases and other important files have been encrypted!

To decrypt your files you need to buy the special software — «Cerber Decryptor».

All transactions should be performed via *bitcoin* network only.

Within 5 days you can purchase this product at a special price: **B1.250 (≈ $041)**.

After 5 days the price of this product will increase up to: **B2.500 (≈ $1882)**.

The special price is available: **04. 23:58:33**

**How to get «Cerber Decryptor»?**

1. Create a Bitcoin Wallet (we recommend Blockchain.info)

2. Buy necessary amount of Bitcoins

   Do not forget about the transaction commission in the Bitcoin network (= **B0.0005**).

   Here are our recommendations:

   - btndirect.eu – A good service for Europe
   - bittlicious.com – Get BTC via Visa / MC or SEPA (EU) bank transfer
   - localbitcoins.com – This service allows you to search for people that want to sell Bitcoins directly (WU, Cash, SEPA, PayPal, etc).
   - cex.io – Buy Bitcoins using Visa / Mastercard or Wire Transfer.

Payment methods: Western Union, Bank of America, cash.
How to get «Cerber Decryptor»?

1. Create a Bitcoin Wallet (we recommend Blockchain.info)

2. Buy necessary amount of Bitcoins

   Do not forget about the transaction commission in the Bitcoin network (= ¥0.0005).

   Here are our recommendations:

   - btcdirect.eu – A good service for Europe
   - bittylicious.com – Get BTC via Visa / MC or SEPA (EU) bank transfer
   - localbitcoins.com – This service allows you to search for people that want to sell Bitcoins directly (WU, Cash, SEPA, Paypal, etc).
   - cex.io – Buy Bitcoins using Visa / Mastercard or Wire Transfer.
   - coincafe.com – It is recommended for the fast and easy service. Payment methods: Western Union, Bank of America, cash through FedEx, Moneygram, and/or wire transfer
   - bitstamp.net – Old and proven Bitcoin dealer
   - coinmama.com – Visa/Mastercard
   - btc-e.com – Bitcoins dealer (Visa/Mastercard, etc.)

   Could not find Bitcoins in your region? Try searching here:

   - buybitcoinworldwide.com international catalog of Bitcoins exchanges
   - bitcoin-net.com – Another Bitcoins sellers catalog
   - howtobuybitcoins.info – International catalog of Bitcoins exchanges
   - bittybot.co/eu – A catalog for the European Union

3. Send ¥1.250 to the following Bitcoin address:

   1DMHu5qcC18NJdbm9zRfsxvQqkzJTV8Gst
I will be sending you details shortly for a professional service expense that needs to go out. Can we process a wire payment for this expense today?

Thanks,

On 2016-10-18 09:31, [Name] wrote:

Will do. Do you have a contract or invoice for this? We will need for documentation in our records.

Below is the account information for the payment of $18,599.00. Code expense to Administrative Expense, Let me know when completed.

Bank Name: Wells Fargo Bank  
Bank Address: 216 Wood Ave. Big Stone Gap, Va. 24219  
Beneficiary Name: Melissa J. Williams  
Beneficiary Address: 180 Light Dr. Dryden, Va. 24243  
Routing Number: 051400549  
Account Number: 8488518385

Thanks,
We will process as quickly as we can.

From: [Redacted]@ku.edu
Sent: Tuesday, October 18, 2016 11:33 AM
To: [Redacted]@ku.edu
Subject: RE: Consulting Expense

I will send all the necessary support for this expense later, Let me know when completed.

Thanks,

On 2016-10-18 09:35, [Redacted] wrote:

We are in process of contacting Commerce Bank to make the transfer. I will let you know when it is complete.
The Beneficiary awaits payment and I will like to know the status of the wire payment. Write back with details.

On 2016-10-18 10:34, [Redacted]

Thanks,

Was this sent as I was walking up to your office?

Our normal contact at Commerce Bank is out so we are trying to contact their assistant to complete the transfer. As I mentioned, we can get it initiated on this end, but it may take a day for it to show up in the recipient's bank. I will keep you posted.

Lawrence, Kansas 66045

From: D [Redacted]@ku.edu]
Sent: Tuesday, October 18, 2016 1:01 PM
To: D [Redacted]@ku.edu>
Subject: RE: Consulting Expense

Can we process and ACH payment for this expense?

Thanks,
Connect with Care

Use common sense when you connect. If you’re online through an unsecured or unprotected network, be cautious about the sites you visit and the information you release.

- Get savvy about Wi-Fi hotspots:
  Limit the type of business you conduct and adjust the security settings on your device to limit who can access your phone.

- Protect your $$:
  When banking and shopping, check to be sure the sites is security enabled. Look for web addresses with "https://" or "shttp://", which means the site takes extra measures to help secure your information. "Http://" is not secure.

- When in doubt, don’t respond.
  Fraudulent texting, calling and voicemails are on the rise. Just like email, requests for personal information or to immediate
YOU SHOULD NOT TRUST PUBLIC KIOSKS WITH YOUR SMART PHONE.

INFORMATION CAN BE RETRIEVED OR DOWNLOADED WITHOUT YOUR CONSENT. LUCKILY FOR YOU, THIS STATION HAS TAKEN THE ETHICAL ROUTE AND YOUR DATA IS SAFE. ENJOY THE FREE CHARGE!

KU Travel Advice

• Take only what you need.
• Remove all unnecessary or sensitive data.
• Encrypt all data, if destination permits it.
• Protect devices from theft.
• Avoid public charging stations, and be careful of open wireless networks

• https://kuit.service-now.com/kb_view_customer.do?sysparm_article=KB0012763
Backup, Backup, Backup!!!

- Carbonite
- CrashPlan
- External Hard Drive
- Network Attached Storage
- MozyHome
- Etc.

http://www.pcmag.com/article2/0,2817,2358135,00.asp
Using Encryption

• Bitlocker
  – Windows 7 Ultimate or Enterprise
  – Windows 8.1 and Windows 10
  – [http://technology.ku.edu/software](http://technology.ku.edu/software)

• File Vault 2
  – OSX 10.7 or higher

**Safely store and preserve the encryption key**

• KU owned devices should use

  Sophos

**IMPORTANT**
Be Aware When Coming Home

• “(B)order agents have a lot of latitude to search electronic devices at the border or take them elsewhere for further inspection for a short period of time, whether or not they suspect a traveler has done anything wrong.”

• https://www.eff.org/wp/defending-privacy-us-border-guide-travelers-carrying-digital-devices
The Worst Security Mistakes Internet Users Make

• Failing to install anti-virus, keep its signatures up to date, and apply it to all files.

• Opening unsolicited e-mail attachments without verifying their source and checking their content first, or executing games or screen savers or other programs from untrusted sources.

• Failing to install security patches—especially for Microsoft Office.
Common Sense is your best defense!

- Don’t reuse passwords
- Use a password manager and 2-step authentication
- Don’t leave your computer unattended, lock Desktop when not in use
- Don’t open unsolicited e-mail attachments from strangers OR your best friend
- Use Firewalls, Anti-Virus Software.
- Patch. Update. Upgrade.

- **Stop and think before you click!!**
IT Security Office

itsec@ku.edu
785-864-9003
security.ku.edu