Cyber Security Awareness Month

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

• Your responsibilities as a KU Employee
  • Data classification and handling
  • KU services and support

• Pros and the CONS of cloud services

• Choosing and using passwords

• Social Engineering, and more
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
Universities Aren’t Safe

- **University of South Carolina**
  81,000 records exposed in 6 separate incidents, 2006-2012

- **University Wisconsin, Milwaukee**
  60,000+ faculty, staff and student records exposed.

- **Univ of Illinois, Urbana-Champaign**
  Students accidentally e-mailed personal information (name, major, gender, GPA, race, et al) on 5,247 students

- **University of Idaho**
  Computers stolen from Advancement Services office contained as many as 70,000 SSNs, names, addresses

Data breach = Data exposure
KU Policy Library

Contains all policies relevant to your employment at KU

http://policy.ku.edu/
KU Privacy Policy

• “Every unit is responsible for maintaining the necessary confidentiality, integrity and availability of the information it handles. Every unit is responsible for granting to assigned individuals within the unit the reasonable, minimum access to Private Information needed to accomplish the necessary institutional purposes.

• All University employees are required to abide by state and federal laws and University policies, procedures and guidelines regarding the handling and protection of Private Information.”
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](#)
## KU Data Classification Policy

<table>
<thead>
<tr>
<th>Confidential Information (level 1)</th>
<th>Sensitive Information (level 2)</th>
</tr>
</thead>
<tbody>
<tr>
<td>KU ID Number + Name</td>
<td>Contract Drafts</td>
</tr>
<tr>
<td>SSN (partial or full) + Name</td>
<td>Checks or Payment Invoices/Tax ID</td>
</tr>
<tr>
<td>Employment Information**</td>
<td>Memoranda</td>
</tr>
<tr>
<td>Individually Identifiable Health Information (IIHI)</td>
<td>Procedures for Managing Accounts</td>
</tr>
<tr>
<td>Litigation Materials</td>
<td>Financial Information</td>
</tr>
<tr>
<td>Student Lists/Rosters Graded Work</td>
<td>Research Subjects</td>
</tr>
<tr>
<td>Credit Card Information (PCI)</td>
<td>Leave Paperwork</td>
</tr>
<tr>
<td>Trade Secret/NDA info</td>
<td></td>
</tr>
</tbody>
</table>
KU Services for KU Data

HawkDrive
hawkdrive.ku.edu

KU Digital Credentials
www.technology.ku.edu/ca/digicert/

KU Data Sharing & Storage Services
technology.ku.edu/services/storage/

KU IT KnowledgeBase
https://kuit.service-now.com/kb_home.do

Microsoft® Outlook® Web App
email.ku.edu

courseware.ku.edu

Secure Jayhawk Wireless
wireless.ku.edu
Living in the Cloud?

- Google Drive
- iCloud
- Dropbox
- SkyDrive
- Amazon Cloud Drive
Losing your “life” in the Cloud

• “In the space of one hour, my entire digital life was destroyed. First my Google account was taken over, then deleted. Next my Twitter account was compromised, and used as a platform to broadcast racist and homophobic messages. And worst of all, my AppleID account was broken into, and my hackers used it to remotely erase all of the data on my iPhone, iPad, and MacBook.”

• http://www.wired.com/gadgetlab/2012/08/apple-amazon-mat-honan-hacking/all/
“As in the great majority of hacking cases, my wife had been using the same password for her Gmail account as for some other, less secure sites, where her username was her Gmail address.”

(Who hasn’t done this?)

James Fallows


Password reuse threatens online banking security

Even IT security professionals reuse passwords – with 81% admitting to risky habit

@SportsLaw_Junky

A Zatik

Found out my #Google account was hacked b/c of the #Trapster app I downloaded & deleted 2 years ago. Just awesome.
KU Password Requirements

- Upper case letters
- Lower case letters
- Digits (0-9)
- Special characters (*, &, %, or $)

- 8 to 16 characters
- If your old password is abcd your new password cannot contain abc, or bcd.
- Wait one year to reuse a password
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/
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

---

![Dashlane Logo](dashlane.png)

![LastPass Logo](lastpass.png)

![SplashID Logo](splashid.png)

![KeePass Logo](keepass.png)

---

[Image of University of Kansas Logo]
Write Down Passwords!!????

However . . .
A paper notebook, kept in a SECURE location, can be an acceptable solution

Umm, NO!
• A thing you know
  • Username, password
• A thing you have
  • Token
  • Code sent to phone or other device

• Services
  – Google
  – Facebook
  – Dropbox
  – LastPass
  – Twitter
“As far as higher education is concerned, the question is not, What information do we have in our databases? but rather, What information don’t we have? ”

Valuable information + a culture of openness and sharing

“Truly, a higher education student database is an identity thief’s dream come true.”

http://www.securityweek.com/higher-education-perfect-security-storm
“Without staff awareness of social engineering scams and techniques, con artists will find the college and university environment an easy target.”
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 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
OK, you got phished . . .

- If you suspect you may have given out your KU credentials, contact the CSC right away, 864-8080.
- Change your password and security questions immediately.
- KU IT will disable (not delete) compromised accounts.
- Check and change passwords to online accounts, such as banks, credit cards etc.
- Inform the police, as well as your credit card providers and banks.
- Consider signing up with a credit monitoring service.
Don’t Ignore Web Warnings!
Phones and Tablets Get Malware too

Infected Devices

All computers

Phones and Tablets Get Malware too
Malware often looks real, like anti-virus software
✓ Don’t reuse passwords
✓ Be aware of social engineering
✓ Lock computer when not in use
✓ Use Firewalls, Anti-Virus Software.
✓ Patch. Update. Upgrade.

Pay attention
IT Security Office
KU Privacy Office
IT Client Services

itsec@ku.edu
privacy@ku.edu
itconsulting@ku.edu

www.besekure.ku.edu