SESSION FOUR

• Ransomware: Legal Issues and Tips to Avoid Being Held Hostage •

• Update on Technology Policies •

• Equity and Access to Technology: Legal and Practical Considerations •

Beware of Ransomware

RANSOMWARE: LEGAL ISSUES AND TIPS TO AVOID BEING HELD HOSTAGE

I. INTRODUCTION

How much would your district pay to get its data back? $600,000? $30,000? $10,000? Ransomware attacks are rampant and this billion-dollar criminal market continues to grow. It is imperative that districts learn about prevention measures such as protocols for responding to an attack and the related legal implications.

II. TERMS / DEFINITIONS

- **Bitcoin:** Digital currency (also called crypto-currency) that is not backed by any country's central bank or government. Bitcoins can be traded for goods or services with vendors who accept Bitcoins as payment.

- **Crypto ransomware**: A type of ransomware that prevents access to files or data.

- **Locker ransomware**: A type of ransomware that denies access to the computer or device.

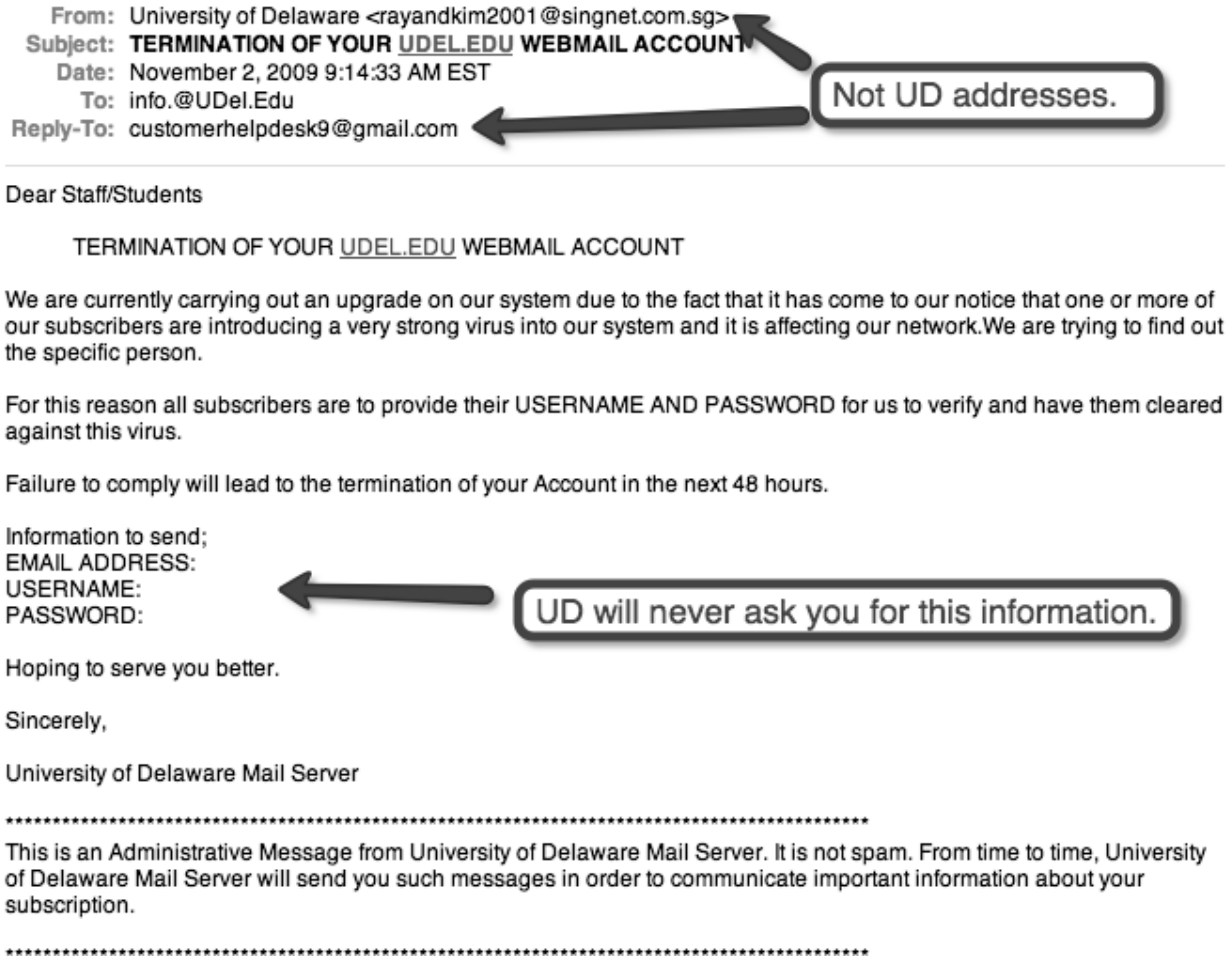
- **Malware**: Software that is designed to disrupt, damage, or gain unauthorized access to a computer system.

- **Phishing**: A form of social engineering that uses email or malicious websites (among other channels) to solicit personal information from an individual or company by posing as a trustworthy organization or entity. Phishing attacks often use email as a vehicle, sending email messages to users that appear to be from an institution or company that the individual conducts business with, such as a banking or financial institution, or a web service through which the individual has an account.

III. WHAT IS RANSOMWARE?

Ransomware is a type of malware. Malware is software designed to disrupt, damage, or gain authorized access to a computer system. Ransomware targets both human and technical weaknesses in organizations and individual networks in an effort to deny the availability of critical data or systems. Ransomware can be introduced by computer and mobile users onto networks through emails, or accessing malicious links and downloads.

Example 1



From: University of Delaware <rayandkim2001@singnet.com.sg>
Subject: **TERMINATION OF YOUR UDEL.EDU WEBMAIL ACCOUNT**
Date: November 2, 2009 9:14:33 AM EST
To: info.@UDel.Edu
Reply-To: customerhelpdesk9@gmail.com

Not UD addresses.

Dear Staff/Students

TERMINATION OF YOUR UDEL.EDU WEBMAIL ACCOUNT

We are currently carrying out an upgrade on our system due to the fact that it has come to our notice that one or more of our subscribers are introducing a very strong virus into our system and it is affecting our network.We are trying to find out the specific person.

For this reason all subscribers are to provide their USERNAME AND PASSWORD for us to verify and have them cleared against this virus.

Failure to comply will lead to the termination of your Account in the next 48 hours.

Information to send;
EMAIL ADDRESS:
USERNAME:
PASSWORD:

UD will never ask you for this information.

Hoping to serve you better.

Sincerely,

University of Delaware Mail Server

****

This is an Administrative Message from University of Delaware Mail Server. It is not spam. From time to time, University of Delaware Mail Server will send you such messages in order to communicate important information about your subscription.

****

Example 2

From: support@ucdavis.edu [mailto:support@ucdavis.edu]
Sent: Sunday, June 16, 2013 11:06 AM
To: support@ucdavis.edu
Subject: Account at Risk

Your Email account is at Risk, follow the link below and sign on to resolve this error.

hold your mouse over the link to see where the link is actually directing you - you should see the link/redirect address

https://cas.ucdavis.edu/login.html

Failure to do so would lead

http://commercialcleaning.kiwi.nz/image/data/davis.htm

suspicious link address

Ucdavis Support

Example 3

IV. HISTORY OF RANSOMWARE

Ransomware originated in 1989 when biologist Joseph Popp introduced the AIDS Trojan. Popp distributed 20,000 infected floppy disks to attendees of the World Health Organization's AIDS Conference. The disks were labeled "AIDS Information-Introductory Diskettes," and included leaflets that warned that the software would adversely affect other program applications, that a user of the disk would owe compensation and possible damages to PC Cyborg Corporation, and that their microcomputer would stop functioning normally. The AIDS Trojan would count the number of times the computer was booted and once it reached 90 it would hide the directories and encrypt or lock the names of files. To regain access, users would have to send $189 to PC Cyborg Corporation at a P.O. Box in Panama.

The world next saw the impacts of ransomware in 2005 when the first wave of modern crypto ransomware appeared with the introduction of the Trojan Gpcoder. Trojan Gpcoder sought out files with various extensions, encoded the files, and then deleted the original files.

V. EVOLUTION OF RANSOMWARE

Since 2005 ransomware has evolved through introduction of new forms almost every year, the most recent being the WannaCry and Petya ransomware in 2017.

Locky ransomware, one of the first evolutions, is spread through spam email messages. Instead of using infected Microsoft documents like previous versions had done, Locky was spread through PDF attachments.[2]

One of the latest versions of ransomware is Popcorn Time. Popcorn Time resembles any other malware in terms of infecting a computer, encrypting its drive, and locking the user out. It differs is that victims can share a link to download Popcorn Time in an attempt to infect others. If two of the victims pay, the attackers give the original victim the free key to decrypt their data.[3]

In May 2017, a new ransomware attack known as WannaCry, or Wanna Crypt, attacked worldwide and affected computers throughout 150 countries. Those victims received messages on their screens demanding a $300 payment in order to have their files restored. This strand of ransomware is similar to the Petya attack that took place soon afterward.

The ransomware Petya is extremely aggressive. The attack caused major companies to shut down their computer systems. Petya attacks the computer, takes over the files and demands $300 in Bitcoins to have the victims' files restored.[4]

[2] http://www.zdnet.com/article/locky-ransomware-is-back-from-the-dead-again-with-new-diablo-variant/
[3] https://www.wired.com/2016/12/popcorn-time-ransomware/
[4] https://www.theguardian.com/technology/2017/jun/27/petya-ransomware-cyber-attack-who-what-why-how

VI. LEGAL CONCERNS

The introduction of ransomware into the educational arena implicated various legal provisions that apply to educational institutions. Some of the statutes that may be implicated in preparing for and responding to a ransomware attack are:

A. Family Educational Rights and Privacy Act (FERPA) 20 U.S.C. § 1232g; 34 C.F.R. Part 99

FERPA is a federal law that applies to educational institutions that receive federal funding (public schools, public school districts, and public colleges and universities). The purpose of FERPA is to protect the privacy of students' education records. FERPA provides that subject to certain exceptions, an educational institution must obtain consent from parents or guardians before sharing students' personally identifiable information. Similar prohibitions appear in state law at Education Code section 49060 et seq. (K-12) and 76200 et seq. (CCD).

B. Health Insurance Portability and Accountability Act (HIPAA)

HIPAA governs the disclosure and use of protected health information (PHI) of covered businesses and their associates. PHI is individually identifiable health information held or transmitted by a covered entity or its business associate, in any form or medium—electronic, paper, or oral. PHI includes demographic data; common identifiers (e.g., name, address, birth date, social security number); information relating to the individual's past, present, or future physical or mental health condition, healthcare provided to him or her, or payment for healthcare; and data that identifies the individual or which could be reasonably used to identify the individual.

HIPAA requires a specific data breach notification process outlined in the HIPAA Security Rule (45 C.F.R. § 164.302 et seq.)

Additionally, the HIPAA Security Rule requires the implementation of security measures to help prevent the introduction of malware, such as ransomware. The required security measures include:

- Implementing a security management process, including conducting a risk analysis to identify threats and vulnerabilities to electronic protected health information (ePHI);
- Implementing security measures to mitigate or remediate identified risks;
- Implementing procedures to guard against and detect malicious software;
- Training users on malicious software protection; and
- Implementing access controls to limit access to ePHI to only those persons or software programs requiring access.

C. Gramm-Leach Bliley Act (GLBA) 15 U.S.C. § 6801 et seq.; 16 C.F.R. Part 313

The GLBA regulates the disclosure of non-public personal information by financial institutions. Under the GLBA financial institutions have an affirmative and continuing obligation to respect the privacy of their customers and to protect the security and confidentiality of those customers' nonpublic personal information.

Schools and colleges that participate in financial activities are covered by the definition of “financial institutions” in the GLBA. The Federal Trade Commission (FTC) has ruled that colleges and universities that offer education loans (e.g., Perkins and institutional loans) are subject to the provisions of the GLBA. The FTC agreed in May 2000 to consider colleges and universities to be in compliance with the privacy provisions of the GLBA if they are in compliance with FERPA. However, schools remain subject to the provisions of the Act relating to the administrative, technical and physical safeguarding of customer information.

The GLBA requires an information security program to establish standards to:

(1) Ensure the security and confidentiality of customer records and information;

(2) Protect against any anticipated threats or hazards to the security or integrity of such records; and

(3) Protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer.

D. Student Online Personal Information Protection Act (SOPIPA) (California Business & Professions Code § 22584 et seq.)

This California law requires education technology providers to comply with baseline privacy and security protections. SOPIPA applies to information on all K-12 students, regardless of their age. Since July 1, 2017, SOPIPA’s provisions also apply to preschool and prekindergarten student’s information

SOPIPA adds the following requirements:

1. Operators cannot target advertise on their site, service, or application or any other site, service, or application using information acquired from students;

2. Operators cannot use information, including persistent unique identifiers, created or gathered by the operator’s site, service, or application, to create a profile for a student, except for school purposes;

3. Operators cannot sell a student's information;

4. Operators cannot disclose student information, unless for legal, regulatory, judicial, safety, or operational improvement reasons;

5. Operators must protect student information through reasonable security procedures and practices;

6. Operators must delete school- or district-controlled student information when requested by schools or districts; and

7. Operators may disclose student information: when required by law; for legitimate research purposes; or for school purposes to educational agencies.

E. California Education Code Section 49073.1

Education Code Section 49073.1 permits public school districts to enter into contracts with third parties for the following purposes:

1. To provide services, including cloud-based services, for the digital storage, management, and retrieval of pupil records; and

2. To provide digital educational software that authorizes a third-party provider of digital educational software to access, store, and use pupil records.

All third party contracts for those technology services must contain the following terms:

1. A statement that pupil records continue to be the property of and under the control of the school district;

2. A description of the means by which pupils may retain possession and control of their own pupil-generated content, if applicable, including options by which a pupil may transfer pupil generated content to a personal account;

3. A prohibition against the third party using any information in the pupil record for any purpose other than those required or specifically permitted by the contract;

4. A description of the procedures by which a parent, legal guardian, or eligible pupil may review personally identifiable information in the pupil's records and correct erroneous information;

5. A description of the actions the third party will take—including the designation and training of responsible individuals—to ensure the security and confidentiality of pupil records;

6. A description of the procedures for notifying the affected parent, legal guardian, or eligible pupil in the event of an unauthorized disclosure of the pupil's records;

7. A certification that a pupil's records shall not be retained or available to the third party upon completion of the terms of the contract and a description of how that certification will be enforced (this requirement does not apply to pupil-generated content if the pupil chooses to establish or maintain an account with the third party for the purpose of storing that content, either by retaining possession and control of their own pupil-generated content, or by transferring pupil-generated content to a personal account);

8. A description of how the district and the third party will jointly ensure compliance with FERPA; and

9. A prohibition against the third party using personally identifiable information in pupil records to engage in targeted advertising.

F. California Constitutional Right to Privacy

The state Constitution gives each citizen an inalienable right to pursue and obtain privacy:

> All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and privacy. (Cal. Const., art. 1, § 1.)

G. California Data Breach Notice (Civil Code § 1798.29)

California law requires a business or state agency to notify any California resident whose unencrypted personal information, as defined, was acquired, or reasonably believed to have been acquired, by an unauthorized person. Civil Code section 1798.29 requires state agencies, including school districts and community colleges, to disclose certain security and data breaches, and specifies notice requirements. Disclosure of a data breach must be made "in the most expedient time possible and without unreasonable delay," and the security breach notification must meet the following requirements:

> (1) notification must be written in plain language, titled "Notice of Data Breach," and present information under the following headings: "What Happened," "What Information Was Involved," "What We Are Doing," "What You Can Do," and "For More Information." Additional information may be provided as a supplement to the notice.

> (2) The format of the notice must be designed to call attention to the nature and significance of the information it contains.
>
> (3) The title and headings in the notice must be clearly and conspicuously displayed.
>
> (4) The text of the notice and any related notice must be no smaller than 10-point type.

A model security breach notification form is prescribed in the statute. Use of the model form or use of the headings described above with the required information written in plain language, deemed to be in compliance with the law.

H. California Anti Phishing Act of 2005 (Business & Professions Code § 22948 et seq.)

In an attempt to crack down on phishing attempts, including unsuccessful ones, the California Legislature passed the Anti Phishing Act of 2005. This law makes it illegal to use email, a webpage, or the Internet to try to induce another person to provide certain information (including social security numbers, credit card numbers, passwords, etc.) by masquerading as a business.

The Anti Phishing Act states:

> It shall be unlawful for any person, by means of a Web page, electronic mail message, or otherwise through use of the Internet, to solicit, request, or take any action to induce another person to provide identifying information by representing itself to be a business without the authority or approval of the business. (Bus. & Prof. Code § 22948.2.)
>
> There are no criminal penalties for violating the Anti Phishing Act. However, violators may be sued in a civil action by either a person harmed by the violation or the California Attorney General.

I. California Penal Code Section 523

In September 2016, the California Legislature passed Senate Bill 1137, which updates Penal Code section 523 to further address the evolution of ransomware. Under section 532, the use of ransomware is punishable by two to four years in prison. Section 523 defines ransomware as:

> computer contaminant or lock placed or introduced without authorization into a computer . . . which the person responsible for the placement or introduction of the ransomware demands payment . . . to remove the computer contaminant . . . .

VII. IMPLICATED DISTRICT POLICIES

The following district policies should be considered in preparing for and responding to a ransomware attack:

- Record Retention Policies
- Technology Use Policies and Acceptable Use Agreements
- Bring Your Own Device Policies
- Student Discipline Policies
- Employee Discipline Policies

VIII. BEST PRACTICES AND TAKEAWAYS

Given the potentially devastating impacts of a ransomware attack, the best defenses are knowledge, vigilance, and preparation. A response plan should include coordination between multiple departments of a district typically Technology, Risk Management, Human Resources/Student Records, and Campus Security.

No institution is immune from attempted ransomware attacks, but these measures can help avoid a successful attack or, at least, limit the resulting damage:

A. Preparing for a Ransomware Attack

1. Educate and Train Employees and Students

    - Do not open attachments from unknown sources
    - Beware of attachments with *.exe* on them
    - Beware of phishing emails
    - Highlight vulnerabilities of peer-to-peer file sharing
    - Make sure important information gets backed up
    - Use the same precautions on your mobile phone as you would your computer
    - Teach good security habits including:
        - Password best practices
        - Protocols for ransomware response

2. Work with vendors that understand the district's responsibilities for data security.

3. Know your data, what it includes, where and in what format it is maintained.

4. Keep a central list of data providers, software vendors, etc. and their key contact information.

5. Identify your response team.

6. Create a written response plan.

7. Consider insurance options ahead of time; be sure cyber insurance policies cover ransomware attacks.

8. Conduct an inventory and identify vulnerabilities.

9. Know your resources (e.g. local authorities, law enforcement, FBI and cyber insurance).

10. Review and update applicable policies and procedures.

B. Responding to a Ransomware Attack

1. Investigate immediately to determine the source and scope of the attack.

2. Shut down systems as needed to prevent further damage.

3. Communicate with staff to contain the spread of the attack.

4. Notify and consult with counsel to determine notification and other legal requirements.

5. Notify law enforcement.

6. Contact insurance carrier(s) to determine coverage and available resources.

7. Work with data storage vendors and software providers to preserve as much data as possible.

8. Consider consultants (IT, PR, forensics, security) to help manage the details and recover data.

9. Notify affected individuals pursuant to statutory notice requirements.

10. Keep a log of the unfolding situation to review when the crisis is over as a learning opportunity for future incidents.