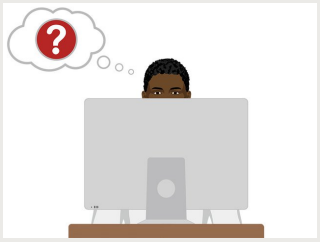
UNC | SCHOOL OF DENTISTRY
Computing and Information Systems

**November/December 2018**

# OUCH! NEWSLETTER

## Am I Hacked? *and* Yes, You Are a Target



This month's newsletter is a double header! First, we find out **how to know when you have been hacked**, and what should you do?

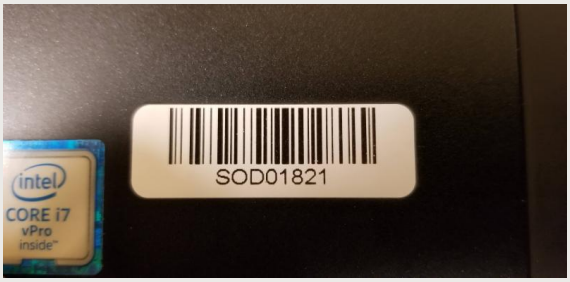
Then, we explain why **you are a target**, how you and your accounts have value and just as importantly what you can do to protect yourself. To subscribe to the OUCH newsletter or view archived articles, **click here.**

## Security Awareness Training Test Requirement

In order to comply with HIPAA and UNC-CH policy, OCIS is enforcing the annual School of Dentistry Security Awareness Training requirement.

You will be **required** to take and pass both the HIPAA and Security Awareness test in

## Laptop Encryption Status




It is not enough for your laptop to be encrypted, we must have documentation and proof of encryption in the event your laptop is lost or stolen.

OCIS is responsible for keeping documentation on the encryption and security of all laptops accessing patient data. If your laptop does not have a tag like the one above, we may not have a record of it. Please bring your laptop to OCIS immediately for a laptop security check.

**REMEMBER: If you have an unencrypted laptop or unencrypted USB flash drive and are using it at the school, contact OCIS as soon as possible!**

***Failure to do so is a violation of HIPAA and University policy.***

## Phishing

OCIS still receives reports of phishing attempts. **To better spot phishing, click here.**

Please forward any phishing messages

order to access the EPR.

To take the Security Awareness Training and Test **please click here.** If you have questions, please contact OCIS.

## How to Create a Secure Password

Your password is your defense against cyber-criminals. It is important that you choose a long and strong password that cannot be easily cracked. This is especially important for in health care environments like the School of Dentistry.

**Click here for the OCIS recommended guidelines for choosing an effective password.**

## Password Managers

A password manager helps to generate and retrieve complex passwords, potentially storing such passwords in an encrypted database or calculating them on demand.

When selecting a password manager for your personal use, **the UNC-CH Information Security Office recommends**

that you encounter **as an attachment** to **phish@unc.edu**.

For an explanation of how to forward an email as an attachment **please read the following article on help.unc.edu.**

To check and see if you have a suspected phishing email, go to **its.unc.edu/phish-alerts/.**

## US DHHS Office of Civil Rights in Action

The US DHHS Office for Civil Rights, reached a settlement with Allergy Associates of Hartford of $125,000 to settle HIPAA violations. In February 2015, a patient of Allergy Associates contacted a local television station about a dispute with Allergy Associates' doctor. The TV reporter contacted the doctor who disclosed the patient's protected health information to the reporter. **Click here to read more.**

Advanced Care Hospitalists (ACH) agreed to pay $500,000 to the Office for Civil Rights (OCR) to settle HIPAA violations. Between November 2011 and June 2012, ACH engaged the services of First Choice Billings. On February 11, 2014, a local hospital notified ACH that patient information was viewable on the First Choice website, including name, date of birth and social security number. ACH was able to identify at least 400 affected individuals. OCR's found that ACH never entered into a business associate agreement with First Choice and failed to adopt any policy requiring business associate agreements until April 2014. Although ACH had been in operation since 2005, it had not conducted a HIPAA risk analysis or implemented security measures or any other written HIPAA policies or procedures before 2014. **Click here to read more.**

you use the matrix given here to evaluate the relative strength of any password manager under consideration.

### ATTENTION: Two-Step Authentication is here!

2-Step for Office 365 is now being fully enforced at the School of Dentistry. If you are having any problems with your 2-step please contact OCIS or ITS. To set up your 2-step, go to https://its.unc.edu/2-step/.

## HIPAA Security Incident Update

The School of Dentistry has gone **112** days since the last reported HIPAA security incident.
**Please stay vigilant!**

### OUCH! Archives

Click here for prior issues and topics.

## Security Awareness Tip of the Day

Remember, it is your personal responsibility to protect patient data (e.g., electronic Protected Health Information) on laptop computers and portable media devices (e.g., CD/DVDs, USB keys, USB drives and SD cards). In all cases, patient data can never be stored on a portable computing or media storage device unless it has been inventoried, encrypted and approved by OCIS.

## Contact Us


**School of Dentistry HIPAA Security Officer**
David Rankin
Email: david_rankin@unc.edu
Phone: (919) 537-3485

**School of Dentistry HIPAA Privacy and Risk Management Officer**
Martin Folliard
Email: mfolliar@email.unc.edu
Phone: (919) 537-3444

**School of Dentistry Deputy Security Officer**
Mauricio Tavares
Email: mtavares@unc.edu
Phone: (919) 537-3428

**School of Dentistry Risk Management Officer**
Martin Folliard
Email: mfolliar@email.unc.edu
Phone: (919) 537-3444


## For More Information

School of Dentistry Policies | UNC-CH Policies | What is Sensitive Information?

(919) 537-3500
OCIS-Help@ unc.edu
http://bit.ly/UNC-OCIS