UNC | ADAMS SCHOOL OF DENTISTRY
Computing and Information Systems

November/December 2019

OUCH! NEWSLETTER

Shopping Online Securely

At last, the holiday season is here!

Black Friday may have come and gone, but millions of more transactions are to be completed for Christmas gifts.

Many of us will be looking to complete our shopping online to avoid the crowds! However, cyber criminals are looking to mark off some items on their shopping list at your expense.

They can do this by setting up fake online stores and setting up scams on legitimate online stores.

Learn more about how to avoid falling victim to these tactics here.

Messaging / Smishing

If you haven't heard it before (in this case many of you have), phishing attacks are the most common tactic that is used to trick or scare users into giving up information.

However, technology is continually changing.

Adversaries are constantly trying new methods to harvest data from end users like us.

These new tactics are spreading across platforms like text messaging, iMessage, WhatsApp and even Skype.

Learn more about how to protect yourself from these types of attacks here.

Security Awareness Training Test Requirement

Laptop Encryption Status

All UNC-CH health affairs schools have a **new IT Security Awareness training** , accessible via SelfService on ConnectCarolina. This training **replaces** all old security awareness training. *Even if you have taken the old training, you will need to complete the new training when contacted by the University's ITS.*

When it is time to take the new training, you will receive an email from Information Technology Services with the subject "Security Awareness Training" and a return address of noreply@unc.edu. Instructions will be included in the email.

Questions? Contact the ITS Service Deck at (919) 962-4357.

Two-Step Authentication

2-Step for Office 365 is now at the UNC-CH Adams 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/**.

How to Create a Secure Password

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

Please forward any phishing messages that you encounter **as an attachment** to **phish@unc.edu**.

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

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

To learn how to better spot phishing, click here.

Change to 1-Year Passwords

The University announced a move to 1-year Onyen passwords effective May 13. You will change to a 1-year password the next time your password comes up for renewal on your current cycle.

What to expect
Passwords **cannot**:

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.

OCIS Security Corner

Campus wide, the most common threat to our computers are phishing attempts. An easy way to identify a phishing attempt is the senders email address.

For example, if someone was trying to mimic my UNC email, it may look like: **Samuel.garcia.unc.edu@yahoo.com**.

ITS implemented a new tool into MS Outlook that will activate whenever you reply to a message that is not coming from a UNC email.

In this case, you will see a banner at the top of your message draft: "The following recipient is outside your organization: *<email address>."*

Remain vigilant: carefully read messages, check who the sender is and report the message if there are any red flags. Do not answer questions from unsolicited phone calls that may be asking you for payment information or to verify your sensitive information such as your SSN.

For more information on how to identify a scam call, **read these tips** from FTC.

Welcome, Sam!

Sam is the Adams School of Dentistry's newest IT Security Analyst.

He is from

- Contain common words or phrases linked to UNC (no more references to Carolina, UNC, Tar Heels or your Onyen)
- Be reused for four years
- Include strings from your previous password (Ex: password1# changing to password2#)
- Be in a database of previously hacked passwords

User interface changes
When you change your password, a strength meter will give you an indication of how strong your password is.

Click here for more details.

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 use, **the UNC-CH Information Security Office recommends you use password managers from well known and established companies.**

ITS is working on something exciting regarding an Enterprise wide password manager for campus.

More information to come!

Fredericksburg, Texas and has been worked in IT Security for over 6 years in the military and private industry.

His hobbies include running, reading and spending time outdoors!

HIPAA Security Incident Update

The School of Dentistry has gone **53** 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

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

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

Adams School of Dentistry IT Security Analyst
Samuel Garcia
Email: **spgarcia@email.unc.edu**
Phone: (919) 445-2877

For More Information

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