University of California San Francisco

Inside this issue:

Ransomware: Practical Tips

You've seen the recent ransomware headlines, such as WannaCry, that impacted organizations across the world. This article will give you information on ransomware and what you can do to protect yourself and UCSF against it.

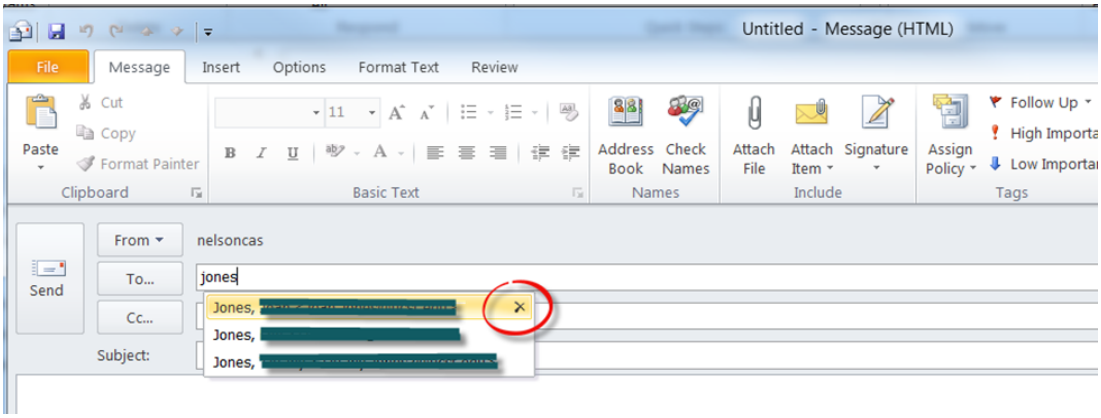
Ransomware is a type of malicious software that locks the victim out of their computer or files – often by encrypting them – until a ransom is paid. Gartner analysts estimate that there were between 2 million and 3 million successful ransomware attacks in 2016 and that the frequency will double year over year through 2019. Ransomware is now a billion dollar industry. Hospitals have been particularly vulnerable to this class of malware.

UCSF has taken a number of precautions to protect against ransomware, notably, the implementation of FireEye, a security technology that helps identify malicious behavior on the network so IT can contain threats as quickly as possible. However, there are still many things you can do to help mitigate the impact of a ransomware attack. *Continued on Page 2.*

Helpful Tip: Reducing Misdirected Emails

MS Outlook is a useful tool that we often use every day. However, it can unwittingly assist in sending an email to an unintended recipient, increasing the risk of exposing sensitive UCSF data (e.g., PHI, PII, etc.) and potentially causing a privacy breach. Outlook remembers every address you have typed into a To, Cc, or Bcc field. This is a good feature: when you start typing in a name or address, Outlook automatically suggests the contact in its entirety. Unfortunately, Outlook remembers all old addresses it has stored, as well as the correct/current one, and can suggest either indiscriminately.

Fortunately, deleting email address entries that you no longer want to appear in the Outlook autocomplete list is easy. First, create a new email message in Outlook. Second, type the name or address you want to remove. Third, delete the undesired email address by using the **down** arrow key (↓) to highlight the entry you want to remove, press the **Delete** button or hover your cursor over the entry you want to remove, and click the (X) that appears to its right.



If you wish to deactivate the Outlook address autocomplete feature completely, click **File** in Outlook. Select **Options**. Go to the **Mail** category. Scroll down to the **Send Messages** section. Make sure **Use Auto-Complete List to suggest names when typing in the To, Cc, and Bcc lines** is not checked. You're done. Note: This helpful tip applies to versions of Outlook from 2010 to present.

If you would like to suggest an error-reducing tip of your own, please email your suggestion to privacy@ucsf.edu.

UCSF Privacy Office

3333 California Street, Suite S1-10G

San Francisco, CA 94118

Box 1922

Phone: (415) 353-2750

Fax: (415) 353-9241

Email: privacy@ucsf.edu

http://hipaa.ucsf.edu

Ransomware (continued from Page 1)

Below are some practical tips to protect yourself and UCSF against ransomware:

- If you receive a ransomware popup or message on your device alerting you to an infection, immediately disconnect your device from the network (unplug wall connection or turn off Wi-Fi) and any external drives to prevent additional infections or data loss.
- Report the incident to the UCSF IT Service Desk by calling 415-514-4100.
- *Install security and anti-virus software.* Be sure to install the UCSF Security Suite on every computer you use for UCSF work, even if you personally own the device. The Security Suite includes our free anti-virus software, Symantec Endpoint Protection – a critical defense against ransomware. The Security Suite also includes BigFix which will assure your computer is patched regularly with the latest security updates.
- *Always ensure your critical files are backed up and stored remotely.* You can do this by using UCSF's back up service, CrashPlan Pro, to back up the data on your device. It is offered at no additional charge to all ITFS supported desktops and laptops as part of ITFS Basic Support and to all UCSF Medical Center supported laptops. UCSF staff, faculty, and students can purchase a CrashPlan subscription for personally owned computers at a discount.
- *Exercise caution.* Don't click on links inside suspicious emails and avoid suspicious websites. If your computer does come under attack, use another computer to research details about the type of attack, but also be aware that the bad guys are often devious enough to create fake sites to tout their own malicious antivirus software or de-encryption program.

If you follow these recommendations and back up, verify, and maintain offline copies of your personal and application data, ransomware attacks should have limited impact on you. With good backups, if you are targeted, instead of worrying about paying a ransom to get your data back, you can simply have your system wiped clean and then restore your files from the backup.

If you have any questions about ransomware, visit the UCSF IT website at http://it.ucsf.edu/ or call the UCSF IT Service Desk at (415) 514-4100.

48 Hours to Report a Research Privacy Incident

Potential breaches of privacy or confidentiality of study participants' Protected Health Information (PHI) or Personally Identifiable Information (PII) are considered "major reportable incidents" that must be reported to the HRPP/IRB. The IRB collaborates with the Privacy Office to investigate these incidents to meet state and federal regulatory obligations in a timely fashion and to avoid penalties and/or late reporting fines for UCSF.

Therefore, Principal Investigators must submit a Protocol Violation/Incident Report Form in iRIS within 48 hours of their first awareness of a violation or incident involving a breach of privacy or confidentiality involving PHI/PII.

Some examples of major incidents involving privacy or confidentiality include the following:

- Failing to properly execute a HIPAA Research Authorization Form due to:
  - Missing a participant's signature or date
  - Missing initials next to an information type in Section C that has been or will be accessed by the research team
  - Accessing items in Section B that are not approved for access or release by the participant
- Failing to obtain a properly executed Consent Form due to missing a participant's signature or date
- Mailing, emailing or otherwise communicating identifiable study participant information to an unauthorized individual (e.g., incorrect participant, incorrect mailing address, incorrect e-mail address, etc.)
- Failing to redact identifiable study participant information sent to a study sponsor (only if the IRB Application and consent form require de-identification)

If you have questions about reporting a research incident involving privacy or confidentiality, contact the IRB at 415-476-1814 / IRB@ucsf.edu or Privacy at 415-353-2750 / privacy@ucsf.edu. Other protocol violations should continue to be reported within 10 working days of awareness.

Observing Patient Care for Educational Purposes

UCSF is fortunate to have top-tier medical education programs full of students with bright and inquisitive minds who are eager to learn and soak up as much information as possible. This is especially evident in clinical settings where students, residents, interns, trainees and fellows can observe patient care as part of their educational experience. However, even though UCSF is a teaching hospital, observation of patient care for educational purposes is not without limits.

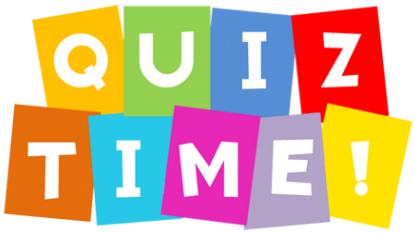
Each patient who receives care at UCSF is required to sign a document called the Terms and Conditions of Services. In this document, the following language is included:

"… Residents, interns, medical students, students of ancillary health care professions… post-graduate fellows, and other trainees may observe, examine, treat, and participate at the request and under the supervision of the attending physician in my care as part of the University's medical education programs."

Patient care and patient safety always come first – it is the responsibility of the attending to ensure that the care environment is well-managed and optimized for patient safety, privacy and confidentiality before permitting observation or participation by students, residents, et al. The attending has the discretion to request that trainees leave the care environment if necessary.

If you have any questions about educational observation of patient care, please consult the attending physician or medical director of your unit for more information.

Test Your Privacy Knowledge — Complete the Quiz



Congratulations to the winner of our Spring Privacy Knowledge Quiz, **Lisa Sears** (UCSF Benioff Children's Specialties). We hope you enjoy your Amazon gift card!

Test your privacy knowledge! For your chance to **win a $25 Amazon gift card**, submit your answer to the question below to UCSFPrivacyOfficeDrawing@gmail.com by **August 15, 2017**. One lucky winner will be chosen out of the correct responses to receive the gift card.

True or False: Accessing UCSF email is not considered "UCSF work," so if you access your UCSF email on a personally-owned device then you are not required to encrypt it.

UCSF Privacy Office Leadership Announcement

After serving as UCSF's Chief Privacy Office for fifteen years, Deborah Yano-Fong, RN, MS, CHPC, has retired from UCSF. We wish Deborah well on her retirement — she will be sorely missed!

The interim Privacy Office leadership is comprised of two Co-Chief Privacy Officers, Michelle Nash, MPH, CHPC and Tom Poon, CIA, CHPC. Michelle and Tom welcome the UCSF community to reach out to them with any privacy concerns and/or questions.

- Michelle Nash: michelle.nash@ucsf.edu | (415) 353-3077
- Tom Poon: tom.poon@ucsf.edu | (415) 476-4405

Upcoming Event: Sharecase@UCSF —Oct. 12th

Come and connect with your peers while learning about the newest collaborative tools, applications, software, and mobile options to simplify your workday.

Our theme this year, "IT Ecosystem: Success through Collaboration," highlights how IT collaborates across the enterprise, working with our partners to develop innovative technologies, and technology based solutions, with the aim of improving patient care at UCSF and advancing health worldwide.

Add Sharecase to your calendar

Key Dates

July 28:
Call for proposals opens
Expo registration opens

August 7:
Attendee registration opens

August 22:
Deadline to submit session proposals

September 15:
Deadline for Expo registration

October 12:
Sharecase@UCSF!