

# National Cybersecurity Awareness Month

National Cybersecurity Awareness Month



OCTOBER 2016

WEEK 2

## CYBERSECURITY '101 Break Room to Board Room

Phishing is a real threat in the healthcare industry. Did you know that a medical record is worth more on the black market than a credit card number? That's because medical records are filled with lots of valuable information that can be used far more broadly than a credit card.

Anyone at IHS can be a target to a scammer seeking PHI (protected health information). Whether you're in housekeeping, nutrition, clinical, or IT, you could be targeted because of your connections to healthcare.

From the break room to the board room, IHS must stay vigilant against phishers.

Don't get hooked! And report 'em if you see 'em!



**Tuesday morning at Townsville Health Service Clinic 8:00AM: Herb & Mel speculate over a suspicious socialite. Credibility of MyFace Friend comes under question.**

So I say to her, "I don't know why that movie star came in to the clinic, I'm just a handy man!" Now she won't message me anymore. It's almost like that was the only reason she sent me a friend request.

Wow, Herb! She sounds like a spy or something!

Well, she's Harry's friend now. I told her he probably knows a lot more since he talks to the doctors and helps them with IT issues.



**10:00AM: Mel & Harry commence coffee-break commentary. The shady lady's plot begins to emerge.**

Herb told me about that crazy MyFace spy! Are you still talking to her?

Who? Ms. Wiley? She's not all bad. She showed me a web download that would clean my PC for free! It worked great! Now I just need to figure out why my password isn't working.

Er... No one else finds this phishy?



**2:00PM: Harry and the doctor see signs of a slip-up. What caper is this culprit trying to carry out?**

I can't seem to access the medical file on my top secret celebrity patient. I even followed the link to immediately verify my username and password like your IT Group email instructed me to do. Can you guys recover lost files?

Er... What email is she talking about? Something smells phishy...



**4:00PM: The phishy data breach pays off! The afternoon news notifies the whole neighborhood!**

The clinical director said they didn't know how the hacker got in to the shared files because they were password protected.

You know, Mel in Housekeeping mentioned something about a wily MyFace trickster trying to con Herb out of patient information.



## NCSAM TIPS OF THE WEEK

Even if you don't have a social media account, your friends probably do. And they might be posting about you! Everyone has an Internet presence, so you can't necessarily hide from scammers, but you can stay alert to prevent potential trouble.

- Be conscientious about whose friend requests you accept on social media.
- Don't always trust that the person on the other end is who they say they are. Spearphishers gain info about your work - even email contacts - and use it to gain your trust.
- Check with IT staff before downloading software on your work computer. Use common sense rules about visiting websites.
- Always be wary of links and attachments in unsolicited emails. Confirm the delivery with known senders.
- When you suspect something may be amiss, email CSIRT@IHS.GOV.