Cybersecurity 101

A National Cybersecurity Awareness Month message,
brought to you by the Division of Information Security

Information Security is an important consideration for everyone these days—especially for people who work in the healthcare industry. Regardless of the vocational duties assigned, as IHS information system users you are responsible for protecting patient and personal information.

Cybersecurity! It's For Everyone! *Even non-security roles.*

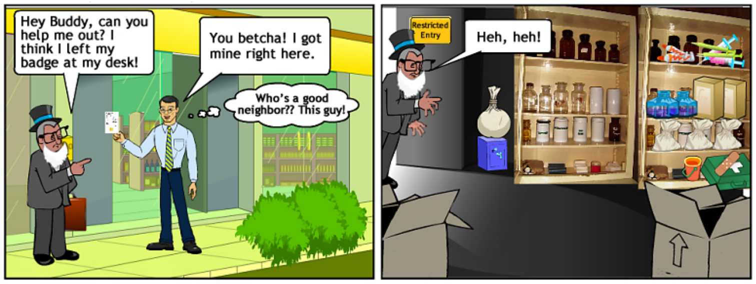
A major threat to information security across the healthcare industry is user exploitation. Crooks use social engineering tactics to get people to provide them with unauthorized access. Phishing is a type of social engineering—often through an email or telephone scam—that tricks users into disclosing sensitive information. Phishers pretend to be affiliated with a legitimate organization in order to gain and exploit login credentials, patient or employee account information, computer hardware data, and more.

Take a look at the Niceguy brothers, whose day-to-day activities don't seem like security risks, but who are nevertheless prime targets for social engineers. The Niceguy brothers have all worked at the same hospital for years, and they know everyone and everything about the place.

Meet Mikey Niceguy...

Mikey Niceguy arrived at work early in the morning and headed toward the restricted employee's entrance in the back of the building. He saw a guy he'd seen a couple times before (he thought his name was Nick), patting his pockets, looking for his badge. Nick asked if Mikey could help him out with the door, and of course Mikey obliged. Who hasn't been in that position?

BUT WAIT! Once inside, Nick was able to continue his social engineering tactics on other unwitting staff, tricking them into believing he was a common employee who'd left his badge at his desk. A few minutes later, No-good Nick could be seen trying to get into the pharmaceutical closet!

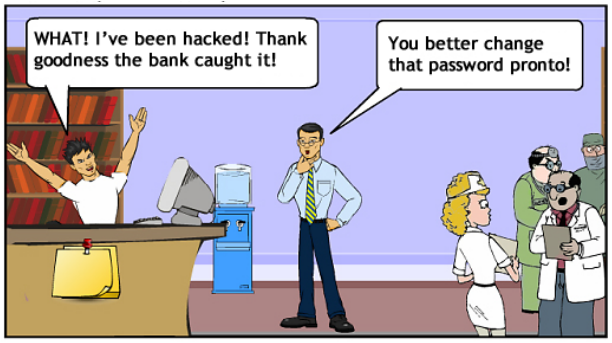

Hey Buddy, can you help me out? I think I left my badge at my desk!
You betcha! I got mine right here.
Who's a good neighbor?? This guy!
Restricted Entry
Heh, heh!

Social engineers are tricky! Don't be fooled into lending your special access to others...even people you think you know.

Meet Jimmy Niceguy...

Later, Mikey stopped in at the nurse's station to see if his brother Jimmy Niceguy wanted to get lunch. Jimmy was obviously shaken up by an email he received from his bank. "Oh my lands!" he said, "someone hacked into my bank account and I have to reset my password immediately!" He clicked on the link and provided his banking username and password to reset it as prompted. Whew! That was a close call.

BUT WAIT! Jimmy didn't validate the authenticity of that link. In fact, he just provided his authentication information to some scammers using a phishing attack! These scammers can now use his information to steal his identity and bleed him dry.


WHAT! I've been hacked! Thank goodness the bank caught it!
You better change that password pronto!

Always be leery of emails prompting you to provide your authentication information, and never click links inside such emails unless you're certain the URL is legitimate.

Cybersecurity 101

A National Cybersecurity Awareness Month message,
brought to you by the Division of Information Security

Meet Joey Niceguy...

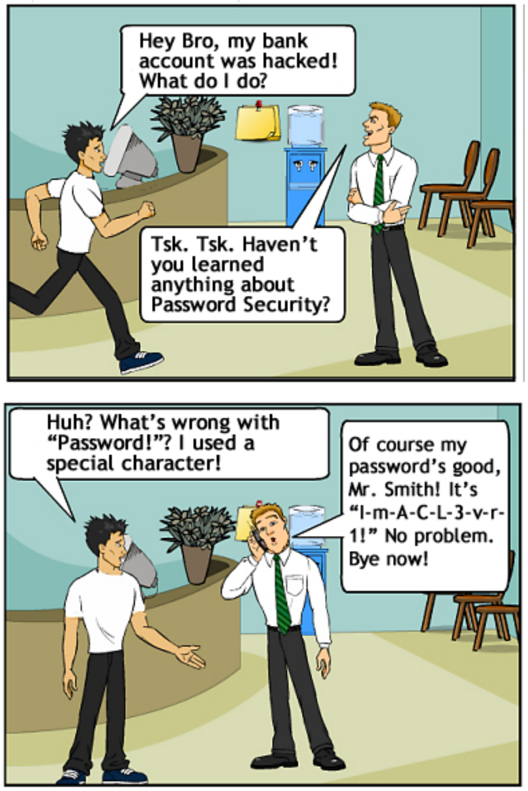
Jimmy raced to see his older brother Dr. Joey Niceguy, who always gave wise advice. Dr. Joey was chastising him for using a weak password when the IT department phoned to make sure his password met complexity requirements. He proudly provided his own password and told Jimmy that he should take a lesson in password security.
BUT WAIT! Dr. Joey just fell for a sophisticated spear-phishing trick! The spear-phisher on the other end specifically targeted this organization's individuals for its information. Now the crook can access electronic medical records and other systems the doctor uses! This is bad news for the hospital, which is going to have some explaining to do!

October
National Cyber Security Awareness Month
staysafeonline.org

Don't get phished.

No one, not even your IT staff or supervisor, will ask you to provide your password.

If someone does, be very suspicious!


Hey Bro, my bank account was hacked! What do I do?
Tsk. Tsk. Haven't you learned anything about Password Security?
Huh? What's wrong with "Password!"? I used a special character!
Of course my password's good, Mr. Smith! It's "I-m-A-C-L-3-v-r-1!" No problem. Bye now!

Meet Danny Niceguy...

And then I'll say, "But wait! There's more!"
Hmm. Yes... Very good.
Oh goodie! The CEO wants my opinion! Let me just download this product detail...
Thanks for the tips, Joey!
Good luck with your proposal!
Hehe. Sucker!

Later that afternoon, Dr. Joey was giving advice to his brother Danny Niceguy, regarding the proposal Danny would give at his executive meeting. Danny received a high-priority email that seemed to come from the CEO. It requested his immediate review and recommendation of a new budget-management product. Danny clicked on the website link and followed the prompts to download a presentation on the software. What a great opportunity for Danny to show off his expertise to the CEO!

BUT WAIT! Danny just fell victim to a sophisticated social engineering attack! This phishing attack spoofed an organizational email and directed him to a phony website where he downloaded malicious software! Be alert with hyperlinks and validate their legitimacy before clicking.

Always be on guard when it comes to downloadable and executable files. Even files that seem benign can be hiding malicious software.