“Locks Keep Out Only the Honest”

Some people think security is just another way of annoying people. Well, it is, but we do have our reasons for annoying…uh, sharing security ideas and notices with you. A lot of you may not know how simple, personal work habits can have a devastating impact on someone’s life or their institution’s reputation, until it does. Let’s hope it never happens; it takes a lot longer to clean up an identity theft than it does for someone to steal the identity and to restore public trust in your institution once it is lost.

The old proverb, “Locks keep out only the honest,” is true physically and virtually. Physically, how secure is your house? You have deadbolt locks on all the doors, keep the windows locked, and your security system armed when you are not home. That is enough to discourage a casual thief, but what about that career thief. That career thief will find a way in; locked windows can be broken; deadbolts can be jimmied; security systems can be disabled or made to appear unreliable; and pets are mostly just pets, not guard animals. Our horses are a bust when it comes to home security; they will sell us out for a carrot or an apple, and help you haul the heavy stuff to the truck.

What about the virtual side of life; are you any safer? One of my favorite responses to our advocating cyber vigilance is:

“Why do we have to worry with that? It’s not like we are guarding nuclear secrets.”

Try this for an answer – FERPA, the Family Educational Rights and Privacy Act!

Okay, how about this for a headline in the local newspapers, and on the AP wire:

“Massive data breach at <insert your favorite institution> *while employee updates their status in Facebook, while still logged into* <insert your favorite internal resource>*”*

With all the security and policies you can think of applied to your computers and network, you will never keep 100% of the bad people out 100% of the time. Just like with your home, you can keep the casual, inexperienced thief out, but that career thief will find a way in, especially when you have a large number of people with computers attached to a network. You may not be able to keep that professional thief out, but you can minimize what they can do; if it isn’t available, it can’t be stolen, if it isn’t accessible, it can’t be accessed.” Here are a few things you can do to slow the thief down and make them work harder:

- Password – have one, make it strong, use it, do not share it, and DO NOT have it written down close to your workstation. We can still turn keyboards over, look on the back of monitors and find the pet, spouse, or favorite child’s name that some use for a password. Make this a really difficult lock for the thief to pick.
- Lock up – when you are away from your computer, lock it (Windows key + L, if you are not familiar with that, Ctrl + Alt + Del and select “Lock this computer”). When you come back you will have to enter your password, but you will have kept the casual thief out.
- “Got access?” – some have too much. Ask and give only what is absolutely necessary, not convenient. Too often, it is easier to grant someone access to data than take the time and respond to the request for information. Some of us also feel we should have access because we

think we should have access. After all, isn't it more "convenient" for everyone involved if I can just access and see everything for myself instead of you having to do it?

- Log out – when you no longer need to access an online source (Banner, Blackboard, bank account, Facebook, etc.), log out of it. If a thief compromises your computer, everything you have access to is also available to the thief.
- PII – personal identifiable information is always sensitive, especially if it is someone else's. How much is too much? You may ask yourself, "what can a thief possibly do with this little bit of information?" You may think they cannot do a lot, but what if you have some of the puzzle, a colleague at the next desk has some, and another office down the hall has some more. If you all had the right pieces, the thief could have a complete puzzle. Don't have it if you don't need it. If you do need it, use the tools available to access it rather than making a comprehensive list to store on your computer.
- Don't stockpile OLD reports with PII on your unencrypted computer or network drive – this goes back to; if it isn't there, it cannot be stolen. The older the reports, the more likely it will contain way too much PII, and they may also contain social security numbers! If you need these reports, save them on an encrypted drive.
- Don't stockpile NEW reports with PII on your unencrypted computer or network drive – again, if it isn't there, it cannot be stolen. If you need these reports, save them on an encrypted drive.
- Don't email unencrypted reports or data containing PII – a couple of things you have to ask yourself before hitting the send button; how strong is my email password (fluffy02 is not strong) and what is the likelihood of the message being intercepted? A best practice is not to send anything sensitive that you do not want to share with the world. If you must, encrypt it. It may not be convenient, but it is safer.

Cybersecurity is a two-way street. You are just as responsible for the data you have and have access to as the IT department. You share the same responsibilities as the IT department for ensuring the data you has meets the three conditions below:

- Data remains confidential – only those authorized can see it
- Data integrity remains intact – only those authorized can change it
- Data remains accessible – those that need access can access it

Cybersecurity is a burden to be shared by everyone, not just the geeks!

Be Safe Out There!