

TECHNOLOGY INSIDER

Protecting Your Password

by **Kristin Beasley of Beasley Technology**



I received a Facebook message from a friend a couple of weeks ago. It said, “Hey, your booty looks great in this video. Check it out!” It was accompanied by a link, supposedly to a video of my booty. I immediately recognized this for a scam, since 1.) My friend does not HAVE a video of my booty; 2.) If she DID have a video of my booty, she would not send me a message about it on Facebook. She would say to herself, “Oops! Someone accidentally focused the camera on Kristin’s booty! I’d better delete that video,” and 3.) My friend would NEVER use the word “booty.”

So what would have happened if I had clicked on the link? The same thing that happened to my friend. The link would open up a way for a “bad guy” somewhere to hijack my Facebook password and send out similar links to all of my friends, who would be left to wonder what in the world I was doing talking about their posteriors, and would click the link and get hijacked, and on and on and on.

I called my friend and told her to change her password, and to stop clicking on links in Facebook, especially ones that included the word “booty.” But the whole situation started me thinking about all the things in our lives that have passwords, and how little care we often take with them. I’d like to offer you a little advice on how to protect your password.

First, we’ve all been told NEVER to write down passwords. We’ve also been told never to use the same password for multiple websites. We’ve also been told to create complex, hard-to-figure-out passwords. The result is that we have 15 difficult passwords to 15 different sites and can’t remember any of them. One of our techs sent me a recommendation for solving this problem. He suggested that you come up with a pattern, or “algorithm,” that you always use for your passwords. For example, your algorithm could be to remove all vowels and add the last



four digits of your parents’ phone number to the end. Using this algorithm, if you wanted to use the word “Tigers” as your password, it would become Tgrs9685. The thing is, you can use a different base word for each password (Rnbws9685 for “Rainbows,” or pgnp9685 for “pigpen”), and you can write that word down. Then you just apply the algorithm every time. The key here is to choose a fairly complex algorithm—for example, adding 123 to the end of a word does not make for a very safe password. But if you choose a good algorithm, then a thief who found your list of base words would never be able to use them to figure out your password.

Whew! Are you still with me? Read it again—it’s a great tip! And it’s not every day you get to use the word “algorithm.”

One final tip, to which I alluded earlier: don’t click on random links. Whether they are in e-mail or on Facebook or anywhere you communicate with people, just ignore them. If they are legitimate and important, the person who sent them will eventually say, “Hey, did you look at that video I sent you?” To which you can reply, “No, I was afraid it might be a virus used to hijack my password. Can you send it again?” And if a message supposedly contains a link to a video of your booty?..... Just leave it alone!