Password Safety

Top Ten Tips for Teens

Sameer Hinduja, Ph.D. and Justin W. Patchin, Ph.D.
Cyberbullying Research Center

1. Never, ever give your password (on Facebook, MySpace, World of WarCraft, the Playstation Network, email, or any similar service) or cell phone unlock code to a friend. Friendships sometimes don't last, and that password or PIN can be used against you.

2. Remember your secret answer. When you create an online account, and it asks you to provide an accurate answer to a question you should know - don't treat it lightly or as a joke. Make sure it's something you will remember months and years from now in case you have a problem at that time.

3. Do not use passwords based on personal information (your login name, birthdate, address, phone number, middle name, pet's name, etc.).

Voices of Victims

Someone has hacked my email address and has changed my password, my personal information and my secret question. I can't log into my own email account! Please help me recover my password. Please rescue me.

4. Use a mixture of upper- and lower-case letters, numbers, and nonalphabetic characters (symbols) if possible.

5. Change your password often. It takes time and is a bit of a chore, but do it anyway. It takes more time and is more of a chore to try to recover from a hacked account or from identity theft.

6. Never provide your password over email or in response to an email request.

7. Make your own acronym by creating a phrase that means something to you, and group together the first letter of each word. Use numbers and symbols when you can. Make sure the acronym you create has at least seven characters. For example:

- "Last week I fell down thirty stairs" (Lw1fd30$)
- "It's 3am, I must be lonely" (I3amimbL)
- "My boyfriend got me a dog for Christmas" (mBFgm@d4C)
- Use short words separated by characters (d0g%d00r, c@ndystr1p).

8. Do not place a written copy of your password on the side of your monitor, under your keyboard, under your mousepad, etc. Figure out a secure place where you can store the passwords you write down – or, if possible – never write down any passwords; it is best to commit them to memory.

9. Do not type passwords on computers that you do not own, control, or fully trust. Computers in Internet cafés, computer labs, airports, libraries, or similar public places should only be used for anonymous Web browsing, and not for logging into your online accounts.

10. Don't use the same password across all of the online accounts you have. Try to use different passwords at different sites, so that one hacked account doesn't lead to other accounts being hacked.

Sameer Hinduja, Ph.D. is an Associate Professor at Florida Atlantic University and Justin W. Patchin, Ph.D. is an Associate Professor at the University of Wisconsin-Eau Claire. Together, they lecture across the United States on the causes and consequences of cyberbullying and offer comprehensive workshops for parents, teachers, counselors, mental health professionals, law enforcement, youth and others concerned with addressing and preventing online aggression.