Tips for Teens: Password Safety

Keeping Your Identity and Information Safe and Secure

Sameer Hinduja, Ph.D. and Justin W. Patchin, Ph.D.

April 2013

1. Protect them

Never, ever give your password (on Facebook, Instagram, Skype, email, or any similar service) or cell phone unlock code to anyone—even a friend. Friendships sometimes don't last, and that password can be used against you.

2. Remember your secret answer

When you create an online account, and it asks you to provide an 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. Don't disclose information about you

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

4. Mix it up

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

5. Be creative

When creating a password, make your own acronym from 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. Here are some examples:

- "Last week I fell down thirty stairs" (Lw1fd30$)
- "It's 3am, I must be lonely" (I3amimbL)
- "Baby you were born this way, Gaga#1" (BuwbtwGAGA#1)

6. Change it up

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.

7. Don't send it to others

Never provide your password via a text message or over email or in response to a request. You could accidentally send it to the wrong person or that person might show it to someone else. Or it could be a scam.

8. Don't post it

Do not place a written copy of your password on the side of your monitor, under your keyboard, in your laptop case, 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 or use highly-rated password manager software.

9. Avoid entering on untrusted devices

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

10. Use different passwords

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 and abroad 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. The Cyberbullying Research Center is dedicated to providing up-to-date information about the nature, extent, causes, and consequences of cyberbullying among adolescents.

For more information, visit http://www.cyberbullying.us.