Tips for Teens: Password Safety

Keeping Your Identity and Information Safe and Secure

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

I. PROTECT THEM. Never, ever give your password (on Instagram, Snapchat, Xbox Live, Fortnite, 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" (LwIfd30$)

"Kiki, do you love me? Are you riding?" (Kdylm@yr)

"May the force be with you!!!" (MtFbWu!!!)

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, or in a DM, or in a screenshot, 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, in your laptop case, in your phone's Notes, 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 apps/software.

9. AVOID ENTERING ON UNTRUSTED DEVICES. Do not enter passwords on devices that you do not own, control, or fully trust. Computers and tablets in school labs, airports, libraries, your parent's office, or other 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 compromised as well.

CYBERBULLYING
RESEARCH CENTER