# StoryPass – Password Rules Hidden in a Storytelling Game Activity: Steps towards Its Implementation

Lamprini Chartofylaka, Antoine Delcroix

# StoryPass - Password rules hidden in a storytelling game activity

## Steps towards Its Implementation

Lamprini CHARTOFYLAKA, Antoine DELCROIX
*Centre de Recherches et de Ressources en Éducation et Formation (CRREF), Université des Antilles*

Abstract
Today, many children are born into a digital culture, accessing new technologies on a daily basis. As a result, within the last few years, experts have been developing numerous tools and practices for education practitioners, parents and children, in order to help the latter adopt a safe online behaviour and grow as responsible digital citizens. A major defining characteristic of digital citizenship (according to ISTE Standards) is password security. As past research shows, children shape their habits by observing (imitation) and recognizing patterns within their experiences (induction), it is essential to design learning experiences which help them understand password issues from an early age. StoryPass is an (offline) game activity prototype which aims to sensitize young children to the need to keep their information private, using strong passwords for their log-ins and sign-ups. Capitalizing on knowledge gained in the area of password robustness and entropy, the game activity idea uses a creative storytelling method in an attempt to deepen children's understanding of password security issues. This paper discusses the first findings from the design and the actual implementation of this learning experience (LX) by students from a Guadeloupe primary school.

Keywords: passwords, storytelling, digital citizenship, children, learning

## Once upon a time...

To date, children in different parts of the world are often described as being "digital natives" (Prensky, 2011), having access to electronic devices and the Internet on a daily basis. Addressing issues about the ethical and safe use of digital media is a collective responsibility to be shouldered by a wide range of stakeholders (parents, teachers). Active mediation and adult supervision have numerous benefits for reducing children's exposure to technology-related risks (Duerager et

al., 2012). Children enhance their knowledge of the world and shape their habits from an early age through observations (imitation) and recognizing patterns within their learning experiences (induction) (Whitebread et.al, 2013). From this perspective, it is essential to acknowledge their tendency towards non-responsible use of media and design initiatives and teaching practices which develop a better understanding of the digital universe.

The ISTE (International Society for Technology in Education) standards for students (2016), promote digital citizenship education as being of great importance. Similarly, the project "StoryPass" is developed around some key components of digital citizenship and identity (standard 2d)[1], for example, personal data management, security settings, and password information. Humans tend to generate their passwords by following specific patterns, such as easy-to-remember passwords, usually based on their personal information and preferences, and those patterns raise several issues concerning usability and security (Biddle et al., 2012). In line with previous studies (Assal et al., 2016, Cole et al., 2017) which revolved around password authentication systems, it is notable that creating a secure password and recalling it may be a challenging learning task for children. Young learners, but also the case for adults, usually create passwords which include personal information (Maqsood et al., 2018), for example, their names, birthdays, pets' names and the like. Other studies and as well as general password strength rules, in particular for human generated passwords, indicate that the use of one-time passwords (Summers et al., 2004), the avoidance of dictionary words and the replacement of letters with other characters (Hu, 2018) are, in a way, efficient solutions for optimizing password security. Where possible and taking into consideration all the aforementioned guidelines, this paper proposes a novel strategy-didactic experience for accessing issues and challenges in developing responsible digital citizenship. "StoryPass" is designed to validate playful (school) interventions and reach groundwork for future studies in digital security education for children.

[1] More particularly, the ISTE standard 2d refers to any efforts which cultivate students' ethical and safe responsibility when using technologies.

## In the beginning there was research design...

### *Materials & methods*

This project utilises an exploratory research approach and aims to evaluate the understanding of children, aged 8+ years old, on several online safety issues and best practices when selecting a secure password. For this purpose, a game was designed as a teaching aid. In its prototype form, the game was tested in a workshop setting, targeting elementary school students. An overview of this workshop is described in more detail in the next section. The core element of this experiment is based on children creating their own story, using the conceptual storyboard schema below.


Figure 1: Storyboard template for inventing a story

From the stories invented, the children were asked to select two notable words extracted from their tale which, in turn, would be used to create their new password. A pseudo-random combination of letters, numbers and symbols is further discussed with the children – before and after – to enable them to enhance and strengthen their passwords. When introducing a safety-oriented protocol to children, with respect to meeting the minimum requirements for creating a strong password, our proposal was based on password related security instructions from the ANSSI Cybersecurity Training Center (Agence nationale de la sécurité des systèmes d'information) (2012). According to ANSSI's official recommendations, setting up a password should be composed of a minimum of 12 different character types, for example:

- Alphabet uppercase letters (A-Z),
- Alphabet lowercase letters (a-z),
- Decimal numbers (0-9),
- Special characters: ~! @#$%^&.

In password generation, issues addressed usually include the ease of which the password may be deciphered – depends on the password's randomness (entropy value) – and the user's recall ability. As these are complex concepts to convey to

children, this project involves the users (children) in the co-creation process rather than directing them to online password generators. The children participate directly in the design of a password, which incorporates their personalised stories. In short, the global research question which encompasses the design phase of this study was "How to sensitize children to IT security in a ludic way?".

## *Step by step implementation*

This section provides an easy-to-use framework for introducing the project concept to young participants.

*Step 1*: In an interactive process, participants received a brief introduction to the realm of passwords and usernames. For example, children were asked the following:

- Do we understand the word "password"? How do we use it?
- What kind of things can we unlock with a password?
- What forms of password are we aware of?

In a metaphorical way, a password was presented as a unique key for unlocking a door to their home and not to be shared with others. During this step, most of the children understood the concept and the usefulness of a password for unlocking a profile, a device, or an account. In addition, their responses were based on passwords which included number and/or letter combinations, in a graphical scheme, similar to a keypad input or fingerprint sensor. The latter two ideas demonstrate a reasonable knowledge (Oliemat et al., 2018), as most of the children are familiar with touch-screen devices (tablets and mobile phones) within their family setting. Subsequently the importance of building secure passwords was highlighted, especially as they may be future users of email accounts, social media profiles, and digital bank accounts. The issue of cyber-security was raised as a potential threat to the protection of their personal sensitive information and their reputation.

*Step 2*: Most of the participants stated their passwords were created from things they knew and loved: their mother's name, favourite singer, date of birth, to name but a few. The children's strategy is well-described and reported in previous studies (for example, Lamichhane at al., 2017). The potential of changing their passwords was introduced through the mixing up words, transforming letters to numbers and combining letters, numbers and special characters (such as @, !, $), as a means of making their passwords more difficult to decipher.

*Step 3*: The general game activity instructions were introduced. Blank story-

boards were supplied to each child. The framework contained six cells and the children were invited to create, step-by-step, a new story from scratch. During the demonstration, each child was individually shown what should be included in each cell, according to the Figure 1. The children were invited to write or draw and the primary motivation was to stretch their imagination in creating a story.

*Step 4*: The children were asked to choose two words from their artwork and record on the back cover of their support documentation.

*Step 5*: After completing this step, the children were asked to make a password out of these two words, by including elements from the things they learnt and retained during Step 2. This was then their new personal password as generated from their whimsical characters and stories.

### *Points of interest*

Coupled with the aforementioned step-by-step framework, it is necessary to highlight the two phases for further analysis.

Phase (a): Children were asked to select two words from their stories.

Phase (b): Children were asked to make a unique word (their new password) by reforming and strengthening the elements of their words according to Step 2.

## In a place, neither near nor far, data found…

### *Participants*

This project was tested with students from a CM2 class (5th grade) at an elementary school in Guadeloupe, French West Indies. The study was conducted with a total of 25 participants, 16 female (F) and 9 male (M), aged 10-11 years.

### *Storytelling productions*

Regarding the means selected to express themselves, 14 students communicated their ideas by writing and 11 chose both writing and drawing. It is notable that all but two participants managed to complete the six elements of the story. The analysis below focuses on the 23 completed story plots. Following are a couple of examples to illustrate the results:

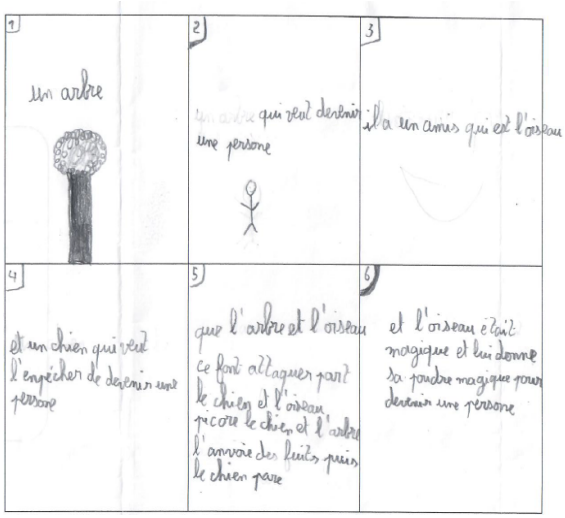


Figure 2: Example of a storyboard (subject n°3)

*There was a **tree (arbre)** who wanted to be a **person (personne)**. He has a friend who is a bird and a dog who wants to prevent it from becoming a person. The tree and the bird are being attacked from the dog. The bird stings the dog and the tree sends its fruits. Then, the dog leaves. And the bird was magic and it gives (to the tree) its magic powder to become a person.*

Password: **@rbrpersonee73**

*Catman wanted to save all cats. His friends are catboys and his ennemis are doggils (waf!). They fight with each other. Doggils die and peace returns for all cats.*

Password: **W@FDOG**

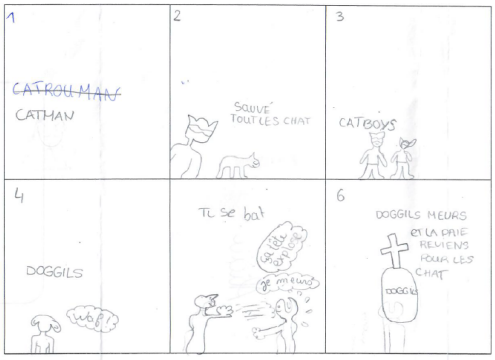


Figure 3: Example of a storyboard (subject n°8)

## And so the analysis goes…

The experimental results showed twenty-three (91%) succeed in providing passwords as requested in phase (b), using words which originated from their story and changing some of the components in accordance with the guidelines provided in Step 2. The two students, who partially completed phase (a), provided a single-word password inspired from their story. A closer examination of their artwork indicated significant differences in the way they applied the rules explained during phases (a) and (b). Interestingly, these outcomes provide a novel framework for further data analysis.

### *Axis 1: Task understanding / Following instructions*

Spanning in detail children's results during the phases (a) and (b) helps us to determine how they interpreted the instructions in order to carry out the learning task. The following table demonstrates how different practices have been employed by the study participants in order to reach the teaching goal, namely, the creation of a robust password. It was developed after examining some tangible results concerning the learning process. More specifically, it was observed whether the participants: (1) delivered a password as requested in phase (b); (2) completed phase (a) before phase (b). In addition, whether the password: (3) stemmed from one, two or more words; (4) included only letters or a combination of letters, numbers or/and special characters; (5) kept the same words during both phases.

| Case # | Phase (a) | Phase (b) | Same word used in both phases | Words | Types [L: Letters, N: Numbers, C: characters] | Number of responses | Examples | |
|---|---|---|---|---|---|---|---|---|
| | | | | | | | **Phase (a)** | **Phase (b)** |
| 1 | ✓ | ✓ | Yes | 2 | L, N or/and C | 9 | poubelledechets | p0belle@dechets377 |
| | | | | | | | Mechanoiseau | Mech@noiseau044 |
| 2 | ✓ ✗ | ✓ | Yes | 2 | L, N or/and C | 3 | !c@pitainspider45. | !spiterd@in45pincs. |
| 3 | ✓ | ✓ | Yes | 2 | L | 2 | miniac catenman | minicatem |
| 4 | ✓ | ✓ | Yes | 1 | L, N or/and C | 3 | HORLOGE | @HORLOGE2008RLA8 |
| 5 | ✓ | ✓ | No | 2 | L or and N, C | 2 | kapten man | KAP-DID-JEUR-BANBINO100 |
| 6 | ✗ | ✓ | - | 2 | L, N or/and C | 2 | -- | @soleiletoile381 |
| 7 | ✓ | ✗ | - | 1 or 2 | L | 2 | chat | -- |

Table 1: Different behaviors on the learning task

As observed from the Table 1, children adapted different behaviours while testing, understanding and learning throughout this teaching game process. Argu-

ably this paper further corroborates the findings of Bloom's Taxonomy of Educational Objectives (Bloom et al., 1956), more specifically on the identified levels of knowledge. Summarizing the seven different cases associated with conceptual understanding and procedural skills of the participants, the results corroborate expected outcomes with respect to factual, conceptual and procedural dimension in the construction of knowledge.

### *Axis 2: Password modelling*

The 21 passwords obtained after phase (b) and analysed below reflect the efficacy of the proposed game activity, in terms of password robustness. With reference to ANSSI criteria previously mentioned, the 21 passwords were more thoroughly analysed.

Firstly, children's preferences for the kinds of characters used for password creation were identified. As anticipated, during phase (a) most of the children wrote using lower case letters. Two participants omitted phase (a) and produced passwords according to phase (b). Within password strengthening recommendations, most of the children preferred to improve their password robustness by adding mostly special characters (such as #, -, @,!) and numbers rather than upper case letters.

Figure 4 focuses on the combination of different character categories used to create passwords during phase (b). One participant provided a password which only consisted of lower-case letters. 12 children combined at least 3 types of characters, for instance:

a) p0belle@dechets377,

b) @soleiletoile381,

c) @HORLOGE2008RLA8.

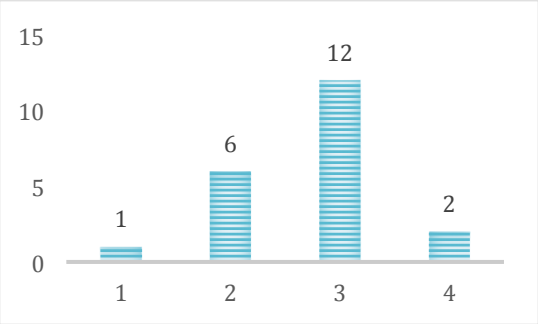


Figure 4: Combination of types of characters

Finally, the length of the passwords created support the view that this pedagogical procedure may assist children produce longer password. 80% of passwords created contained of a minimum of 12 characters.

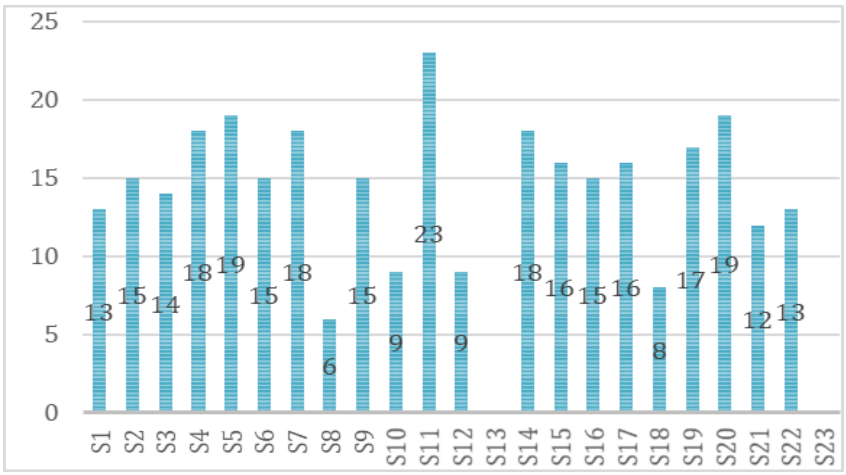


Figure 5: Length of their passwords

## Happily ever after, there is a conclusion…

In the cyber era, personal information must be handled securely. Data security and privacy requires learning digital skills, including basic password management techniques. Teaching children of the importance of online privacy is an issue that needs to be addressed from a young age. In the modern era, some children may have access to digital devices, apps and websites without an awareness of security principles. For those children who will become exposed to a digital world, acknowledging the need for understanding password importance should be embraced in a long-term perspective.

Creating a strong password could be a demanding task and it is necessary that children get into the habit at an early age. In addition, they also need to learn how to safeguard and memorize passwords. However, they are more likely to remember passwords originated from their personal experiences and creations. This paper presents a hands-on approach through which children, while playing, nurturing their creativity and imagination, through a storytelling game activity, may be able to make and manage their own personal passwords.

One of the learning goals of StoryPass is to inspire children to adopt safe online behaviours and to help them understand key elements of creating strong passwords to protect their personal accounts. Despite the fact that the findings presented are based on a limited number of participants, the results are promising regarding establishing a new teaching strategy with respect to increasing children's knowledge concerning password security. The proposal discussed may be successful in terms of its usability, as children repeat the same procedure, creating new

stories thereby updating their frequently used passwords. As Clifford Stoll reputedly said: "Treat your password like your toothbrush. Don't let anybody else use it and get a new one every six months".

## Acknowledgments

The authors would like to thank the study participants, the class teacher, Suzy Luce, and the Primary School Director, Turenne Thénard – Grand Bois, Le Gosier, Guadeloupe – for their invaluable contribution to the author's experience.

## References

AGENCE NATIONALE DE LA SECURITE DES SYSTEMES D'INFORMATION (ANSSI), France (2012): *Recommandations de sécurité relatives aux mots de passe*. Technical report.

ASSAL, H., IMRAN, A., & CHIASSON, S. (2016): An exploration of graphical password authentication for children. *International Journal of Child-Computer Interaction,* 18, 37-46.

BIDDLE, R., CHIASSON, S., & OORSCHOT, P. V. (2012): Graphical passwords. *ACM Computing Surveys*, 44(4), 1-41.

BLOOM, B.S. (ed.) (1956): *Taxonomy of Educational Objectives: The Classification of Educational Goals, by a committee of college and university examiners. Handbook I: Cognitive Domain*. NY, NY: Longmans, Green.

COLE, J., WALSH, G., & PEASE, Z. (2017): Click to Enter. *Proceedings of the 2017 Conference on Interaction Design and Children. IDC '17*.

DUERAGER, A., & LIVINGSTONE, S. (2012): *How can parents support children's internet safety?* EU Kids Online, London, UK.

HU, G. (2018): On Password Strength: A Survey and Analysis. *Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing Studies in Computational Intelligence*, 165-186.

INTERNATIONAL SOCIETY FOR TECHNOLOGY IN EDUCATION (ISTE). (2016): *ISTE standards for students.*

LAMICHHANE, D. R., & READ, J. C. (2017): Investigating Children's Passwords using a Game-based Survey. *Proceedings of the 2017 Conference on Interaction Design and Children. IDC '17*.

MAQSOOD, S., BIDDLE, R., MAQSOOD, S., & CHIASSON, S. (2018): An exploratory study of children's online password behaviors. *Proceedings of the 17th ACM Conference on Interaction Design and Children. IDC '18*.

OLIEMAT, E., IHMEIDEH, F., & ALKHAWALDEH, M. (2018): The use of touch-screen tablets in early childhood: Children's knowledge, skills, and attitudes towards tablet technology. *Children and Youth Services Review*, 88, 591-597.

PRENSKY, M. (2011): Digital Natives, Digital Immigrants Part 1. *On the Horizon*, 9(5), 1-6.

SUMMERS, W. C., & BOSWORTH, E. (2004): Password Policy: The Good, The Bad , and The Ugly. *WISICT '04 Proceedings of the winter international symposium on Information and communication technologies*.

ITEBREAD D. & BINGHAM S. (2013): *Habit Formation and Learning in Young Children*, Report, University of Cambridge.