UgCERT
UGANDA COMPUTER EMERGENCY RESPONSE TEAM

UGANDA COMMUNICATIONS COMMISSION

Password Security, Protection, and Management

Every Password Is Important

With the many ways we use the Internet, it's easy to consider some passwords less important than others. However, all passwords are important because wrongdoers can piece together the information you store online and use it for their benefit. They can even use information you share on social media networks. And commercial websites give customers the ability to store billing and shipping addresses along with credit card information. This paper offers recommendations for protecting your information by selecting strong passwords and storing and managing them safely.

Creating and Protecting Your Passwords

The complex methods that attackers can use to gain access to your personal information are becoming more easily accessible to wrongdoers and are increasingly effective. It is important to avoid the common mistakes that give these individuals the opportunity to exploit your personal data.

Common Mistakes and Remedies

Mistake #1: Using a weak password. Selecting a weak password is like closing your front door but not locking it. A password is weak if it can be guessed easily. Examples of weak passwords are dictionary terms, common phrases, your name or birthday, or "password" and" p@ssw0rd".

Remedy:The easiest way to create a secure password is to use a pass phrase. A good example comes from the Microsoft Safety & Security Centre (italics added):

> Start with a sentence or two. *Complex passwords are safer.*
> Remove the spaces between the words in the sentence.
> *Complexpasswordsaresafer.*Turn words into shorthand or intentionally misspell a word. *ComplekspasswordsRsafer.*Add length with numbers.
> Put numbers that are meaningful to you after the sentence.
> *ComplekspasswordsRsafer2011*.

The Microsoft exercise shows how you can create a passphrase that is both strong and easy to remember. It follows several safe password guidelines: it is long, it is not a common phrase, it includes numbers, and it includes both lower case and upper case letters. The one guideline

missed in the example is to use special characters such as punctuation or, for example, a dollar or pound sign.

Mistake #2: Using the same password for every account. This is a security concern because if an attacker guesses or cracks a password for one account, he or she can access all your accounts. Even if the attacker gets the password for a relatively non sensitive account; he or she can reuse it on sites where, for example, billing, payment, health, and other private information is stored. Using the same pattern for your passwords is also risky. By learning your current password structure, attackers can increase their chances of guessing passwords for critical websites such as your bank account or your company's email account.

Remedy: Use a different password for each website you access. A password manager— essentially an encrypted database— can help you store all these unique passwords and pass phrases in one safe, well-protected place. (See the next section for details about password managers.)

Mistake #3:Exposing passwords to others. This can mean logging in from a public computer, keeping a note with passwords written on it where it can be found, or sharing your passwords with others. It can also mean having your web browser store your password information. If you get a prompt asking if you want a site to remember your password, say "no." The reason is that most browsers store passwords encoded in a way that is publicly known, and thus easy to decode. Password recovery tools, which are easily available online, enable anyone to see all the passwords stored in the browser and open users' profiles.

Remedy:Avoid public computers and public access networks. If you happen to use one, do not access private, sensitive, or business information; and change your password afterwards. In all cases, keep your passwords well protected, perhaps by keeping them in a lock box or safe, or in an encrypted file or password manager. Avoid sharing passwords. Occasionally, you might have a guest who needs access to your home wireless network. Share your *strong* pass phrase only with a visitor you trust, or type it in yourself. (It's common courtesy as well as a good security practice to look away when someone is typing his or her password.)

Password Managers

A password manager is software for storing all your passwords in one location that is protected and accessible with one easy-to-remember master pass phrase. It is one of the best ways to keep track of each unique password or pass phrase that you have created for your various online accounts—without writing them down on a piece of paper and risking that others will see them. When using a password manager, you have one master pass phrase that protects all of your other passwords. This leaves you with the ease of having to remember only one.

With the growing number of necessary passwords and the amount of information that people have stored in online accounts, the Internet is an attractive place for malicious users to steal your personal information. By using complex passwords and pass phrases and choosing a password manager that fits your password use habits, you can keep your information secure and protect yourself from identity thieves.

Before you decide on a password manager, read reviews of the various products in order to understand how they work and what they are capable of doing. Some reviews include both strengths and weakness. Also do your own analysis by reading background information on vendors' websites. When you have chosen a password manager, get it directly from the vendor and verify that the installer is not installing a maliciously modified version by checking an MD5 hash of the installer; if a hash is not available, request one from the vendor; if the vendor cannot

provide a verification method, be sceptical. Although moving to a password manager may take a little effort, in the long run it is a safe and convenient method of keeping track of your passwords and guarding your online information.