DIGITAL SELF DEFENSE:
how to create a secure password

Is your Password Easy to Crack?

If you have forgotten your password or believe it has been compromised, contact the ITS HelpDesk.

get informed
Visit the RIT Information Security website to read the security standards, access security tools and software, or find out more ways to protect yourself.

RIT INFORMATION SECURITY
http://rit.edu/security
infosec@rit.edu
(S85) 475-4123

why use a secure password?
If someone cracks your password, they can:
• Obtain your personal information, which can lead to identity theft.
• Gain access to your e-mail account to read and send e-mail.
• Access MyCourses or other services.
• Access RIT Confidential information on the Institute network.
• Gain information about your registered computers at RIT and register their own on your RIT account.

protect your password
There are several different ways someone can acquire your password:
• **Cracking**: Password cracking programs are designed to guess the most common passwords first. Most current programs can make over one million crack attempts per second.
• **Malware**: Password stealers and keyloggers are often packaged with viruses and spyware. Always run up-to-date anti-virus.
• **Social Engineering**: Never give away your password to anyone, even someone claiming to work for a help desk.
• **Phishing**: No company will ever ask you to confirm your password through e-mail. Never click on links in an e-mail asking you to do so. Type the website URL in manually.

why use a secure password?
If someone cracks your password, they can:
• Obtain your personal information, which can lead to identity theft.
• Gain access to your e-mail account to read and send e-mail.
• Access MyCourses or other services.
• Access RIT Confidential information on the Institute network.
• Gain information about your registered computers at RIT and register their own on your RIT account.

get informed
Visit the RIT Information Security website to read the security standards, access security tools and software, or find out more ways to protect yourself.

RIT INFORMATION SECURITY
http://rit.edu/security
infosec@rit.edu
(S85) 475-4123

DIGITAL SELF DEFENSE:
how to create a secure password

Is your Password Easy to Crack?
what is a secure password?

A secure password should be virtually impossible for others to guess. It should not contain or be based on personal information, and it should not be written down or given out to anybody.

RIT Information Security recommends:
• Minimum 8 characters (longer is preferred)
• Mixed upper and lower case letters
• At least one number and at least one symbol

Minimum requirements for passwords can be found at: https://www.rit.edu/security/content/password

what should I avoid?

There are many ways people try to make their passwords easier to remember. Cracking programs look for the most common passwords first.

Passwords should NOT:
• Contain your RIT username
• Be the same as other passwords you are currently using (including non-RIT services)
• Be a single word, forward or backward, from an English or foreign dictionary
• Contain more than 3 sequential characters on a keyboard (ex: qwerty or 1234)
• Contain more than two consecutive repeating characters (bbbbb2bbb)
• Be all numbers such as birthdates or anniversary dates (ex: 011551)
• Be shared with anyone for any reason

how do I choose an easy to remember password?

Here are three simple ways to construct a secure, easy to remember password:

1. Create a passphrase by choosing a short phrase and:
   • Changing the capitalization of some of the letters
   • Replacing some of the letters with numerical and symbolic substitutions ($ for S, 8 for B)
   • Purposefully misspelling or abbreviating some words
   (E.g.: The phrase “iced tea is great for summer” becomes “!cedTisgr84$umm3R”)

2. Choose several shorter words and add some numbers in the center. Then change the capitalization and substitute symbols for letters. (E.g.: “bO()K451BR^Dbury”)

3. Choose a memorable quote or phrase and use only the first letter from each word. Vary the capitalization. Make sure to also include numbers and symbols, either as substitutions for letters or as a replacement for a full word. (E.g.: “ywAM100%ot$tyN+”)

HINT: You can also use a password safe to generate a random password for you.

the easiest solution: use a password safe

Password safes save your passwords securely, allowing you to save the information on your personal computer without opening yourself up to giving away private information inadvertently. They can also generate random passwords for each of your accounts.

These password safes store all of your passwords in a single account, which has a master password you need to remember. This allows you to use truly random combinations in all of your other passwords, making them much harder for malicious users or bots to crack. Two examples of such services are LastPass and Password Gorilla.

change your password regularly

The RIT Password Standard requires passwords to be changed annually. In addition, passwords should be changed:
• Whenever a malicious program such as a virus is detected or a machine is compromised in some way.
• If there is a job change (job is completed, job is terminated, or a job transfer changes the need for access).
• From any default passwords.
• If they are shared with anyone other than the authorized user(s).

http://rit.edu/security