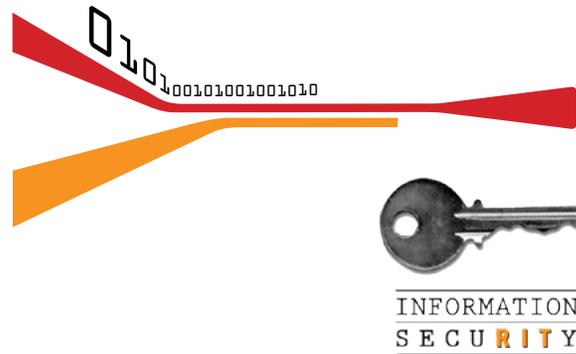


protect your password

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.



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

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

(585) 475-4123



DIGITAL SELF DEFENSE:

how to create a secure password

Is your Password Easy to Crack?



Revised 7/21/2014

