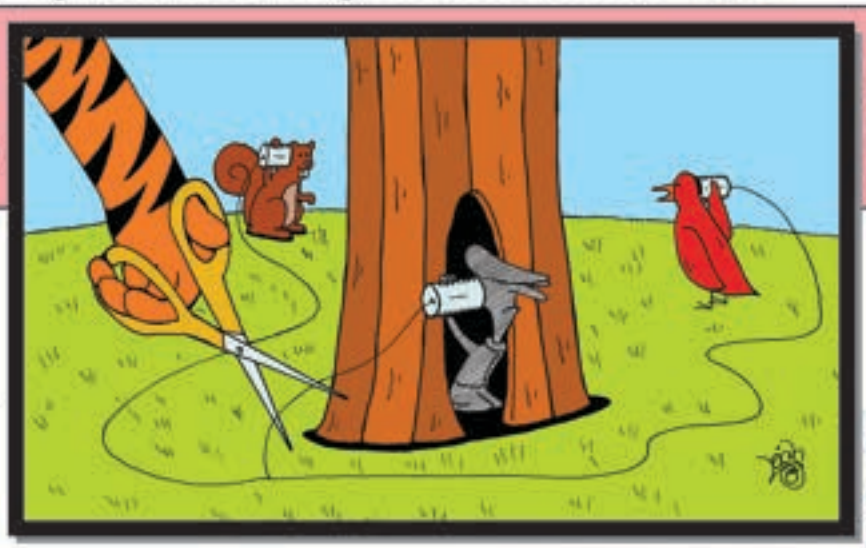
# The Sketchy Cybersecurity News from RIT


**Remember:**
**"If you read it here, it's probably Sketchy!"**



Happy November, Tigers!
Welcome to the second edition of the Sketchy Cybersecurity News from RIT. This month's topic is **Man in the Middle** attacks.

With Thanksgiving, football, family get-togethers, and all of those crazy Black Friday deals, the month of November can get a little hectic! We're here to remind you to stay vigilant online and not fall victim to Sketchy's tricks.

## MITM

**Man in the Middle Attack:** a form of active wiretapping attack in which the attacker intercepts and selectively modifies communicated data to masquerade as one or more of the entities involved in a communication association. The most common MITM attack is when an attacker creates a fake login page for a website you frequently use, directs you to that page through a phishing email, and then steals your information, such as your username, password, or credit card numbers before redirecting you to your intended website.

### Why do MITM attacks still work?

MITM attacks still work because they are based on deception and social engineering. **Social engineering** is a form of manipulation that involves giving up information. Social engineers use various tactics to convince you to click a link directing you to a fake, but familiar looking website. The attack still works because the hacker doesn't break into anything, they just take advantage of your trust though urgency and reasonable requests. Usually, they pretend to be a friend, coworker, or familiar store asking for shipping or payment updates. You might believe it's a reasonable request and in an effort to speed up any delayed processes, give up your sensitive data to the attacker.

### Fun Fact:

The first MITM attack took place in 1903 when Guglielmo Marconi's radio message was intercepted. A skeptic at the time, Nevil Maskelyne sent his own radio message repeatedly encoding the word "RATS" in the recognizable morse code.

To learn more, visit: https://cyber.rit.edu/rats

### How to prevent MITM attacks:

- Be vigilant for phishing emails asking for credentials or other personal info
- Only use known, secure WiFi access points that require specific credentials
- Pay attention to website addresses and any address changes from page to page
- Ensure every website address matches the actual anticipated website names
- Always look for the lock symbol ensuring the website is verified as secure
- Only visit websites with the "https://" in the website address

During the busiest online shopping time, be wary of public WiFi networks as they open you up to MITM attacks. Public networks can expose users to network sniffing. **Network sniffing** is when an attacker monitors network traffic to determine what devices are on the network, what websites people are visiting, and what data they are sending. Malicious attackers commonly use network sniffers to intercept and analyze your private information because public networks usually do not use encryption. With this type of MITM attack, you aren't even aware that an attacker intercepted and stole your personal information. So, please make sure you pay close attention to the website addresses you visit and stay wary of entering your information while on public WiFi, or you may not be feeling very thankful this season!

To protect your online security, visit: https://www.rit.edu/security/online-security



Next month's topic: Online Payment Safety!

This Month's Authors: Eddie DiTomasso, Peiyang Lin, Yahades Peralta, Jon Todd
Sketchy Cybersecurity Editor: Rick Mislan, PhD • RIT Cartoonist in Residence: Leigh Rubin