Army Vision: By 2028, a world-class Army that is a source of national pride.

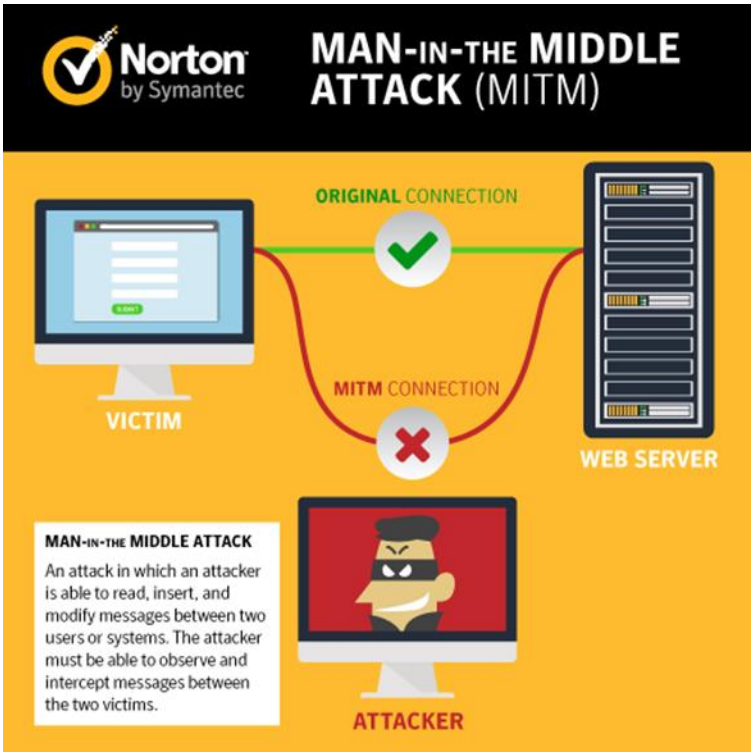
H E A D Q U A R T E R S
P H I L I P P I N E A R M Y
OFFICE OF THE ASSISTANT CHIEF OF STAFF FOR
COMMAND AND CONTROL COMMUNICATIONS, AND CYBER SYSTEMS, G6
Fort Andres Bonifacio, Metro Manila

6/CMB 09 December 2016

CYBERSECURITY BULLETIN

Cybersecurity Bulletin: #75

What Is a Man In The Middle Attack (MITM)?



Phishing is one of the oldest tricks in the Internet book that tries to trick you out of divulging your personal information. This is topic aimed at educating you on how to stay protected on today's Internet landscape.

Phishing is essentially an online con game and phishers are nothing more than tech-savvy con artists and identity thieves. They use SPAM, malicious web sites, email messages and instant messages to trick people into divulging sensitive information, such as bank and credit card accounts, usernames and passwords.

How Do You Know It's a Scam?

There are different forms of phishing tactics. Criminals may try to trick you into giving away your personal information via emails, Social Media messages, IMs, text messages, and even Internet chat rooms. Sometimes criminals may try to fool you into installing a malicious program, known as spyware, which can track and record the information you enter into your computer. Below are some of the commonly used tactics and warning signs you should be on the lookout for:

- Phishers, pretending to be legitimate companies, may use email to request personal information and direct recipients to respond through malicious websites. Phishers have been known to use real company logos, and will also use a spoofed email address, which is an email address that is similar to the actual company's address. However, the address may be misspelled slightly or come from a spoofed domain.
- Emails may come in the form of a help desk support ticket, a message from your bank, or from someone soliciting money via a 419 scam aka Nigerian Scam- like fake lotteries, dying widow scam etc.
- Phishers tend to use a call to action. You may get a notice that an account is being shut down and you need to log into it to avoid that from happening. They may also request personal information in order to verify your identity.
- Phishing websites can look remarkably like legitimate sites because they tend to use the copyrighted images the original sites.
- Fraudulent messages are often not personalized and will often have misspellings of words and company names.

How Do You Know If You Have Spyware?

Spyware can be downloaded from web sites, email messages, instant messages, and from direct file-sharing connections. Additionally, a user may unknowingly receive spyware by installing a software program, and the spyware piggybacks onto that installation as additional suggested software. Users may also be unaware that some browser add-ons contain spyware.

Spyware frequently attempts to remain unnoticed, either by actively hiding or by simply not making its presence on a system known to the user. However, sometimes there can be signs that you may be infected:

- Your computer starts to run slower than usual.
- You start to receive an unusual amount of pop up ads.
- There are new toolbars on your browser that you did not install.

- Your browser's home page has changed to a page that you are unfamiliar with.
- Your web searches become redirected to other spam sites.

How Do I Avoid Spyware?

- Be selective about what you download to your computer.
- Watch out for anti-spyware scams.
- Beware of clickable ads.
- Use Anti-Virus to provide anti-spyware protection and proactively protect from other security risks.
- Do not accept or open suspicious error dialogs from within the browser.
- Spyware may come as part of a "free deal" offer - do not accept free deals.
- Keep software and security patches up to date.

How Do I Protect My Privacy?

If you happen to run across any of these red flags, here are some tips to keep yourself safe and protect your privacy:

- Never give out any personal information via email, social media platforms, text messages or instant messages.
- If the call to action is to click on a link and sign into the site with your username and password, never click on the link. Instead, go to your web browser and type in the website's URL. Be sure to look for the verified https:/ at the beginning of the URL in the task bar.
- Never download a program or file from a suspicious email. These may contain programs such as spyware and keyloggers.

Reference:

This was cross posted from:
https://community.norton.com/en/blogs/norton-protection-blog/how-protect-yourself-phishing-scams

DO YOU WANT TO KNOW MORE? TALK TO US.

POC: LTC JOEY T FONTIVEROS (SC) PA – Chief, Cyberspace Management Branch, OG6, PA at Landline Telephone Nr: 02-845-9555 Local 6630 and Mobile Telephone Nr: 0917-6281057. Email: fontiverosjt@army.mil.ph.