

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

HEADQUARTERS
PHILIPPINE ARMY
**OFFICE OF THE ASSISTANT CHIEF OF STAFF FOR
COMMAND AND CONTROL COMMUNICATIONS, AND CYBER SYSTEMS, G6**
Fort Andres Bonifacio, Metro Manila

6/CMB

27 March 2017

CYBERSECURITY BULLETIN

Cybersecurity Bulletin: #17-12

How to Stay Safe When File Sharing Online



File sharing technology is an easy way for individuals or institutions to transfer content on the internet. There are several peer-to-peer (P2P) applications and services available. Some applications are free and others offer paid subscriptions for larger storage capacity, speedier service or extra security. File sharing is a very common activity for most online users, but file sharing also makes you susceptible to various online threats including identity theft, infection or attack.

If you plan on using file sharing technology, be sure personal data and other sensitive materials are secure and safeguarded before you engage with a file sharing service online. Here are some useful tips to help you understand the dangers of file sharing, and how prevent a malicious attack.

What Are the Risks?

Peer-to-Peer file sharing applications can put your personal information at risk. Most of the time, users are sharing data with people they know or conduct business with. But how can these individuals' identities be validated online? The truth

Cybersecurity Bulletin #17-12

Army Core Purpose: Serving the people. Securing the land.

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

is it's almost impossible to verify a source on file sharing applications, which means the users on the other end may not be who you think they are.

In the case of illegal downloads, like music and movies, users download content without any knowledge of the source. Both of these instances introduce security risks that put you and your personal data in jeopardy.

Attackers use file sharing applications to install spyware, malicious codes, viruses, Trojan Horses, and worms. They do so by bundling the content you desire with these threats. When you download the content, you're inviting in any number of security risks and, without proper safeguards, they can result in any number of security breaches.

Additionally, some file sharing interfaces expose your computer directories without your knowledge, allowing attackers to view information you might not have intended to share. You might also share personal data willingly, and assume it's safe to do so because it's being sent directly to known sources. The security features on file sharing applications won't keep out every criminal, especially because attackers are constantly evolving online. It's never a good idea to share files you would rather keep private.

Finally, some file sharing applications will request open ports on your firewall. Firewalls are designed to encrypt communications going into and out of your computer so attackers can't see what you're sending or receiving. By breaking this barrier to allow content to download successfully, you're putting your computer at risk of attack.

How to Stay Safe

The easiest way to ensure the safety of your personal information while using file sharing applications is to be aware of what you send and what you attempt to download. Don't send highly sensitive material through file sharing services. Similarly, be aware of the content you're downloading. Do not share or download illegal or pirated content. In the event that you are caught sharing or downloading illegal content, even if it's accidental, you might be faced with fines or serious legal penalties. Moreover, using company property to download or share illegal content can result in legal actions and possible termination. Be aware of your actions online and steer clear of dangerous behaviors.

In addition to being vigilant about what you should and should not share via file sharing applications, make sure that your Internet Security software, such as Norton Security is installed, activated, and up to date. Anti-virus software scans your computer for incoming threats and will recognize most viruses, provided it's kept current. Stay on top of this, and it will greatly reduce your chances of enduring an online attack.

Additionally, you should install and enable a firewall. Some operating systems come with a built-in firewall so be sure that it's enabled and working properly. If your computer doesn't have a firewall, make sure to get one before you share or download files on a file sharing application.

File sharing can make our lives a little easier, but only if we take the necessary steps to protect ourselves online. Follow these tips, and you'll greatly reduce your chances of attack, identity theft, or infection.

Cybersecurity Bulletin #17-12

Army Core Purpose: Serving the people. Securing the land.

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

Reference:

This was cross posted from:

<https://community.norton.com/en/blogs/norton-protection-blog/how-stay-safe-when-file-sharing-online>

DO YOU WANT TO KNOW MORE? TALK TO US.

POC: MAJ GIL P TARIO II (SC) PA – Assistant Chief, Cyberspace Management Branch, OG6, PA at Landline Telephone Nr: 02-845-9555 Local 6630 and Mobile Telephone Nr: 0917-7982005. Email: tariogp@army.mil.ph.