East Midlands Special Operations Unit

COVID-19 CYBER AND FRAUD PROTECT MESSAGES

Monday 20 July 2020

This advice has been collated by EMSOU and is intended for wider distribution within the East Midlands Region to raise awareness among businesses and the public.

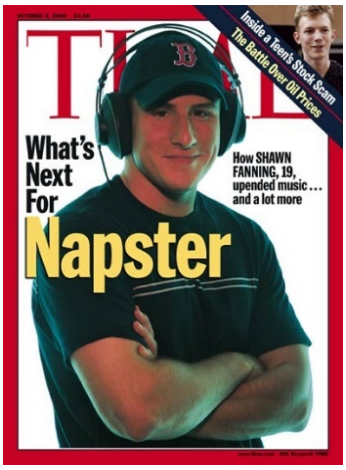
Advice and information is changing daily as we navigate our way through the COVID-19 pandemic, so please ensure you only take information from reputable sources.

If you require any further information, assistance or guidance please contact the

EMSOU Protect Team EMSOU Protect Team **or your local Force protect team.**

Today's topic is: File Sharing

File sharing is a phenomenon as old as the World Wide Web and was quickly exploited by those with criminal interests. As early as 1994, the FBI was raiding the home of Edwina and Eddy Hardenburgh who, between them had over 124 phone lines and hundreds of computers exchanging gigabytes of illegally copied games, hacked software and pornography on a daily basis.



Of course, it took the ever sleepy, Sean Fanning (aka the Napster) and a 1984 court ruling regarding the use of Sony's Betamax tapes and their illicit use of spreading pirated movies, that resulted in the success of the 1999 file sharing platform Napster.

Legitimate file sharing, using Peer-to-peer (P2P) software, is one of the many benefits of using the web. P2P software, which is often free to download, enables millions of users spread across the globe to share music; photos, videos, software, code and an abundance of electronic documents. As with most technology, however, file sharing can put your sensitive data and digital devices at risk.

Criminals and malicious actors are quick to exploit peoples trust and malicious applications and malware can easily be distributed on file sharing platforms and when downloaded by the unwary can have serious consequences.

Security risks from file sharing

- **Malicious Code:** When you use P2P applications, it is difficult to verify that the source of the files are trustworthy. These applications can be used to spread malicious code such as spyware, viruses, Trojan horses, or even computer worms.
- **Exposure of sensitive data:** Using peer-to-peer software often involves opening-up different directories to other people. Any form of compromise or oversight, however, could expose sensitive data such as financial records; medical information, personal documents or corporate files. Of course, once this information has been exposed, it's difficult to know how many people have accessed it.

- **Susceptibility to attack**: Some P2P applications may ask to open certain ports on a firewall to transmit files. However, this may give attackers unauthorised or detected access to a computer system. There are even P2P applications that can modify and penetrate firewalls themselves, without your knowledge.
- **Flawed software:** Peer-to-peer applications - especially the less known products - may also have inherit flaws because of poor coding or software development practices. Adversaries will use these vulnerabilities to launch attacks on any machine participating in file sharing.
- **Denial of service** - Downloading files causes a significant amount of traffic over the network. This activity may reduce the availability of certain programs or limit access to the internet.
- **Prosecution** - Files shared through P2P applications may include pirated software, copyrighted material, or pornography. Downloading these, even unknowingly, may result in fines or other legal action. If the computer is on a company network and exposes customer data then the company may be liable.

Mitigation Techniques

The best way to eliminate these risks is to avoid using P2P applications. If there is a need to use P2P software the following steps should be taken:

- **Use and maintain anti-virus software**: To recognise malware and protect systems against them.
- **Install or enable a firewall**: To block malicious traffic before it enters a system. Be wary of opening ports unless the consequences of doing so are fully appreciated.
- **Look for reassurance**: Does the platform take security seriously? Is the sender known and generally trusted? Are hash values or digital signature included with the download to lend integrity and legitimacy?

Hot Topic:

A recent phishing email trend is targeting job applicants, sending out emails confirming that applicants have been successful in a job application, then asking them to click on suspicious links to view the job offer or terms and conditions.

A new Primark phishing scam was the most frequently reported phishing email in the last week. These emails offer the recipient a reward for “overcoming the coronavirus”. Recipients are asked to click on a link to complete a survey to get their reward.

Reporting

Please report all Fraud and Cybercrime to Action Fraud by calling 0300 123 2040 or online.
Forward suspicious emails to report@phishing.gov.uk.
Report SMS scams by forwarding the message to 7726 (spells SPAM on the keypad)