What Users Should Know About Email Cyberthreats

PART I IN A THREE-PART SERIES FOCUSED ON CYBERSECURITY

Michelle Vayle | RENOVODATA

EFFECTIVE CYBERSECURITY RELIES on good network planning and a range of high-level, protective products. However, some of the most effective guardians of networks and data are users themselves, because they can thwart many of today's email-based threats as well as those on the horizon.

BLUE ISLAND/SHUTTERSTOCK.COM

In the next three issues of *3PL Perspectives* we will walk you through the different types of threats with examples of what to watch out for. We will conclude by describing best practices for protecting your business.

The most frequent entry point for cyberattacks is email, and that is where users stand as the first line of defense. Any email originating outside the organization can contain threats, and genuinely innocent email can be compromised by cyber criminals.

Email fraud seeks to fool recipients into taking unwise actions, so users should be aware of the kinds of threats their inboxes may contain. Continual vigilance is the key. This is especially important for 3PL and trucking companies because of the volume of email involved in day-to-day business and the speed with which users must handle their work.

Below is a list of the most common cyberthreats that all users should know:

Malware is short for malicious software. It is spread by programs that surreptitiously invade computers and launch damaging activities before the intrusion is detected. Its goals can be to steal data, damage data, hold data hostage, spy on users' behavior, take over systems, sabotage systems' key functions, subvert system protections, and any other kinds of mischief that cyber-criminals can devise.

Malware can appear as downloads, email attachments, clickable links in social media, and other forms. Penetration vehicles include viruses, worms, Trojan horses, adware, and spyware.

Viruses are programs that carry specialized malware. They spread by attaching to regular software when a user launches the program. They can also spread through script files, documents, vulnerabilities in web apps, and other pathways. Unlike worms, they almost always corrupt files.

Worms are also vehicles for malware. They take advantage of operating systems' vulnerabilities and cause damage to their host networks – often by overloading their capacities. A major difference is that worms have the ability to self-replicate and spread their poisons independently while viruses rely on human activity, such as running infected programs, for their distribution.

Trojan Horses, aka **Trojans**, are programs that appear to be normal software or files. Perpetrators are highly skilled in making their weapons look harmless. Once a user unintentionally invites a Trojan in by making a mistaken click, the software can seize data such as logins and financial information, steal electronic money, install more malware, modify files, monitor user activity such as screen-watching behavior and key strokes, and much more.

Hackers, many of whom are good guys, are a talented breed of high-end computer programmers who specialize in combing through existing programs to spot hard-to-find problems. **Malware hackers** are computer experts who have put their skills to work for dark purposes. Causing damage via malware is known as hacking and pieces of malware or acts of assault are called hacks.

Normally, a **bug** is simply an unintended error in a program, usually minor. In the hands of malicious hackers, however, a bug is an error created and inserted into victims' programs to do harm. An **exploit** is a software element or command that tells a previously introduced bug what to do to, up to and including seizing control of the targets' computer systems.

Bots are specialized programs designed to do particular things and are valuable tools in the legitimate world of computer technology. However, in the hands of malware hackers bots do bad things, such as send spam and build hostile networks **(botnets)**. They also deliver **spiders**, programs that perform such tasks as harvesting server data and attaching malware to search results.

Rootkit programs allow hackers to control computers remotely and invisibly. They can wreak havoc in many ways, including stealing data, corrupting security software, and taking control of the system as part of a botnet. Because they are so adept at hiding, rootkits are exceptionally hard to detect and can commit deep sabotage before they are found.

Adware delivers advertisements that can be benign nuisance pop-ups, dangerous malware-entry weapons, or something in between. All types promote enticements to purchase something or to receive free software or computer services. Adware tempts victims to act on impulse, and the results can be disastrous.

Spyware, often contained in adware, can capture user information such as logins and passwords as well as account and financial details. It can also steal data. Spyware exploits software vulnerabilities, bundling itself with legitimate software, or combining with Trojans. Spyware can redirect users to fraudulent websites and can capture users' website-visit information.

Phishing uses disguised query emails to extract information from anyone who responds. It employs the technique of **spoofing**, in which mail comes from what falsely appears to be the addresses of legitimate sources, such as social or charity web sites, financial institutions, government agencies, payment processors, or IT administrators. **Spear phishing** takes the scam to a higher level, targeting specific individuals and companies as opposed to the more scattershot approach that snaps shut on any victim who falls for the bait.

ANY EMAIL ORIGINATING OUTSIDE THE ORGANIZATION CAN CONTAIN THREATS, AND **GENUINELY INNOCENT EMAIL CAN BE COMPROMISED** BY CYBER CRIMINALS.

Ransomware, now an epidemic-level cyber security issue, uses invasive encryption techniques to extort money by holding an organization's network and data hostage. Perpetrators demand that victims pay money to regain access to their property or lose it forever. By paralyzing operations, ransomware can inflict severe damage to organizations of any size. Not only is payment a loss of money, it is no guarantee that the kidnapped data will be released. Because 3PL and trucking companies rely so heavily on timeliness, having activities frozen for even a brief period can be disastrous.

These are some of the most prevalent email-related threats users face every day, and such cyberattacks continue to grow, in numbers and ingenuity. Fortunately, the same is true of cyber security providers, whose experts are constantly devising new defenses for new dangers. Solid security-related tools and processes, from firewalls and anti-malware software to data backups and disaster recovery solutions, give strong protection.

Michelle Vayle is Marketing and Sales Director for RenovoData in Atlanta, GA. She may be reached at mvayle@RenovoData.com or 877-834-3684. For a wider range of information on cyber security, go to http://www.renovodata.com/blog/.