your energy partner®
OPPD
Omaha Public Power District

SHIELD
SECURE
HANDLE
INVOLVE
ELIMINATE
LEARN
DEFEND
Information Protection Newsletter

Triple Threat Sucker Punches

You may have heard of the sucker punch, where an attacker punched without warning, allowing no time for the defender to block the punch. Not only does the threat of sucker punches exist in the real world, it is also present in the cyber realm. As an OPPD employee or contractor, you are pummeled daily by cyber-attacks designed to attack systems without warning, and often without initial indications that the attacks are under way.

In these sucker punch attacks there are two main types of malware that cyber criminals attempt to install **Trojan horse** malware is mainly used to steal user IDs and passwords for web sites and online banking. It can also be used to remotely control compromised systems, destroy data, send out spam, or record a user's keystrokes. Another type of malware is called **ransomware**. It can be also be used to encrypt files that can be accessed by the attack victim. The victim is given files containing ransom payment instructions. There are numerous reports of ransomware crippling organizations because critical information essential to their operation has been encrypted.

There are three types of cyber sucker punches to guard against: Web-based drive-by attacks, email-based phishing attacks, and portable media based worm attacks.

Drive-by attacks use a variety of flaws in operating systems, browsers, and browser plug-ins. These flaws can be used to run small programs used to download malware to your system. This process is performed step by step with bits of the malware being loaded until it is complete. The attacks occur when you visit a compromised web site. They can install Trojan horse and ransomware malware.

You can guard against drive by attacks by confining your surfing to business-related sites. This does reduce your chance of being attacked, but even legitimate sites can have compromised software installed. You must also ensure your anti-virus is up-to-date and working, and importantly that your operating system, Internet browser, and browser plug-ins are patched. Exampled of plug-ins include Adobe Reader and Adobe Flash Player.

Phishing attacks make use of messaging technology like email. The messages are crafted to appear like they are from people you know or from legitimate organizations. They often have an element of urgency to encourage the readers to act immediately by either clicking on a link or opening an attached file. The links take your browser to a malicious web site that installs malware. The attached files are really malware files that if installed with compromise you PC. Phishing attacks can install Trojan horse and ransomware malware. Additionally they are used in banking fraud cases where money is transferred to offshore bank accounts supposedly at the direction of a company executive. Your best defense against Phishing attacks is common sense. Stop and think before you act on the phasing email's instructions. Pick up the phone and call the person or contact the organization using its public contact information. Odds are the email is not legitimate.

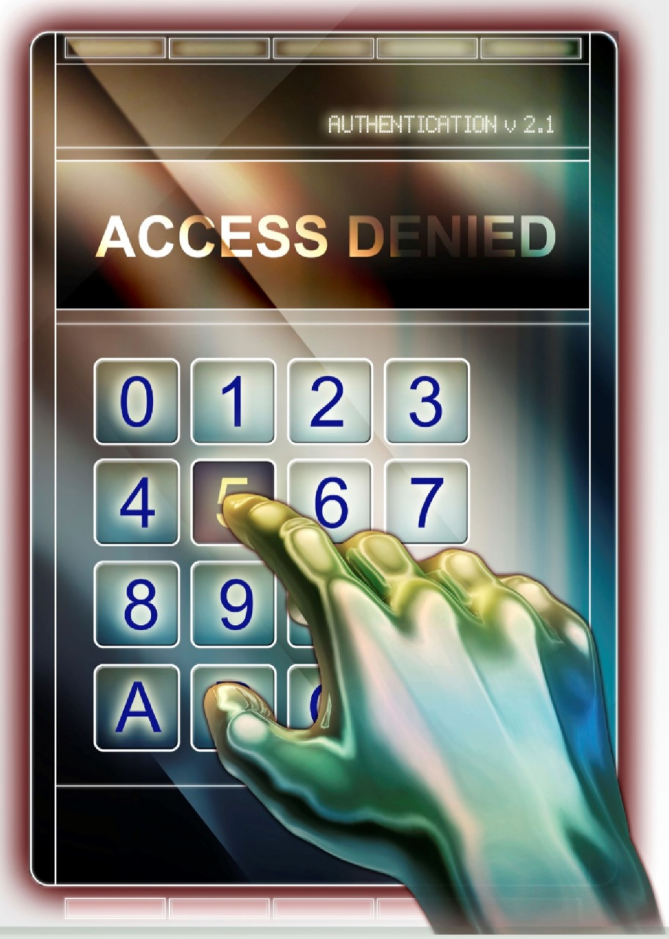
Portable media based worm attacks occur when a user connects a compromised portable media device like a USB thumb drive to a computer. If the computer allows portable media devices to automatically play programs that are often used to install software, the malicious software can be installed. It will perform whatever the malicious installation program directs. Thereafter, the newly compromised system will infect any portable media devices that get connected to it. Portable media worms can install Trojan horses and ransomware. This type of attack is useful against isolated networks that cannot be attacked over the Internet or via email. You can defend against this attack by only using portable media set aside for file transfers. This portable media must also scanned between uses to ensure that it has not been compromised. Consult OPPD portable media procedures to learn how file transfers should be conducted.

Finally, if you believe you've been a victim of one of these cyber sucker punches, please contact your supervisor and the Business Technology Service Desk for assistance. You are our first line of defense against cyber criminals who want to catch us unaware.

Passwords

Your passwords are the keys to your kingdom. Guard them well.

- The longer your passwords are, the better.
- Never share your passwords.
- Use different passwords for different accounts.



your energy partner
OPPD
Omaha Public Power District

This poster is published by OPPD's
Cyber Security & Information Protection Department.
For more information, please contact us at:

BT Service Desk

© The SANS Institute 2014

At home or at work

Safely Working Remotely

You can work from almost anywhere in the world, thanks to today's explosion of Internet devices and connectivity. However, with that convenience comes new security threats through the very devices that make working from home so easy.

If you have been authorized to work from home remember that home networks and Internet connections are not as secure as OPPD's internal network. Connection to OPPD's internal network may be automatically denied if a potential security issue is detected.

Home networking equipment must be properly configured with firmware properly patched. Keeping these home networks updated is the responsibility of the employee or contractor. Using a home Wi-Fi connection is allowed provided the wireless router is configured for Wi-Fi Protected Access 2 (WPA2). Use of a wireless mouse does not pose any significant security problems. However, wireless keyboards might be prone to interception, allowing a nearby attacker to capture what is being typed.

Do not use obsolete operating systems such as Windows XP. Cyber criminals exploit the hundreds of unpatched flaws present in Windows XP, its Internet browsers and browser plugins. Upgrade to at least Windows 7.

Teleworking from public Internet connections should be avoided, since any Internet traffic through these connections is prone to interception. Places of heightened risk include airports, coffee shops, and hotels.

Certain technologies and popular communications applications may not be allowed for teleworking because of security reasons. These include using peer to peer file sharing services and peer to peer chat services. These may be prone to compromise and cannot be guaranteed as being secure.

Please contact your supervisor and the BT Service Desk for any questions about working from home.

OPPD
Omaha Public Power District

This poster is published by OPPD's
Cyber Security & Information Protection Department.
For more information, please contact us at:

BT Service Desk

© The SANS Institute 2014

North American Electric Reliability Corporation Quarterly Update

CIP-003-6 Cyber Security- Security Management Controls

R1. Each Responsible Entity shall review and obtain CIP Senior Manager approval at least once every 15 calendar months for one or more documented cyber security policies that collectively address the following topics:

1.1 For its high impact and medium impact BES Cyber Systems, if any:

1.1.1. Personnel and training (CIP-004);

1.1.2. Electronic Security Perimeters (CIP-005) including Interactive Remote Access;

1.1.3. Physical security of BES Cyber Systems (CIP-006);

1.1.4. System security management (CIP-007);

1.1.5. Incident reporting and response planning (CIP-008);

1.1.6. Recovery plans for BES Cyber Systems (CIP-009);

1.1.7. Configuration change management and vulnerability assessments (CIP- 010);

1.1.8. Information protection (CIP-011); and

1.1.9. Declaring and responding to CIP Exceptional Circumstances.

1.2 For its assets identified in CIP-002 containing low impact BES Cyber Systems, if any:

1.2.1. Cyber security awareness;

1.2.2. Physical security controls;

1.2.3. Electronic access controls for Low Impact External Routable

Connectivity (LERC) and Dial-up Connectivity; and

1.2.4. Cyber Security Incident response

OPPD's NERC CIP Cyber Security Policy represents OPPD's commitment to securing BES Cyber Assets and BES Cyber Systems. The policy identifies OPPD's intent to provide guidance and outlines OPPD's standards which all employees, contractors and service vendors whom are subject to the NERC CIP regulations, must adhere to. The policy outlines requirements such as, OPPD's Personnel Risk Assessment Program, Access Management Program, NERC CIP Security Training Program, Physical Security Plan and OPPD's Cyber Security Incident Response Plan.

t is crucial for all OPPD employees, contractors and service vendors, who are subject to NERC CIP regulations, to understand and to comply with the criteria set forth within the OPPD's NERC CIP Cyber Security Policy. The OPPD NERC CIP Cyber Security Policy can be located at all NERC CIP Physical Access points. For contractors, please contact your OPPD sponsor to attain a copy of the OPPD NERC CIP Cyber Security Policy.

For more information pertaining to OPPD's NERC CIP Cyber Security Policy, please contact , Mike Nickels – (402) 552-5036; manickels@oppd.com or Suzanne Krajicek – (402) 552- 5165; skrajicek@oppd.com .

your energy partner®

OPPD

Omaha Public Power District