USER-CAUSED INFECTIONS

Most ransomware attacks are caused by user-error!

HOW CAN THIS HAPPEN?	HOW DO WE COMBAT IT?
Bad Emails with Phishing & Spearphishing...	**Via anti-spam**
Infected Websites...	**Keeping necessary Windows patches up-to-date and installing firewall**
Bad Websites... *-Such as gambling*	**Content blocking**
Malvertising... *-Infected ads on websites*	**Content blocking and GOIP** *-Blocking unnecessary countries*

WHAT DO THEY DO NEXT?

1. They escalate on a local user to gain admin access to workstations/laptops.
2. They get on the server.
3. With admin-rights on the server, they can gain rights to all machines.
4. They discretely break the back up.
5. They copy the data to the Internet.
6. They spring the ransomware and encrypt your network.

ONCE THEY'RE IN, IS IT A LOST CAUSE?

No! We are monitoring for suspicious activity 24/7. The moment something comes up, we're on top of it. Additionally, by keeping everything up to date, security is top notch.

HOW DO WE COMBAT IT?

- We don't allow users to be admin on the network or workstations.
- We get 24/7 notifications of any suspicious activity on the server, workstations or Office365.
- We install firewall and inspect Internet traffic.
- We lock up backups with separate credentials.
- We block file sharing websites.

PARTNERS P·L·U·S

302-529-3700 www.PartnersPlus.com Hello@PartnersPlus.com