Kevin Wolf

From: info@podi.com
Sent: Tuesday, June 25, 2019 8:02 AM
Subject: PODI News - Ransomware Defenses and a New PayPal Security Feature

PODI dot COM
POTOMAC DIGITEK
online. solved.

Defending Against Ransomware

Have you heard of computer malware called CryptoLocker, WannaCry, SamSam, or NotPetya? Each is a variation of malware called Ransomware.

Ransomware is a type of electronic attack on an organization's networked computers which, once inside the organization's defenses, disables access to each computer. The attacker then offers to restore access if a ransom payment is made. Hackers have been honing their ransomware capabilities and broadening their targets to include businesses, hospitals, and city or state governments.

Some organizations, like the city of Riviera Beach, Florida decided to pay the $600,000 ransom rather than suffer the consequences. Others, like Baltimore City decided to rely on its own resources to remove the malware and recover key governmental functions. To date, the cost of the recovery effort is $18 million and climbing. The success and high visibility of ransomware attacks ensure they will continue.

We urge everyone to take the time to consider their organization's ransomware defenses. Here are some tactics we use to avoid or limit the damage from a ransomware attack.

1. All of our client web sites are hosted on hardened servers that have strong physical and electronic security. The days of self-hosting and casual security efforts are long gone. If your organization struggles to keep up with the latest security imperatives, consider using Managed Service Providers like Design Data , Digital Industry , or DataBank .

2. Train and remind staff to anticipate suspicious emails. Everyone should be on the lookout for suspicious emails and avoid clicking on ANYTHING that looks even remotely questionable. Especially beware of emails with attachments or those that request financial information.

3. Ensure backing up computer files is part of your normal office routine and is done frequently. We use a third-party service called iDrive which is configured to make scheduled backups frequently. Defining a schedule for automatic backups avoids gaps from 'forgotten' or 'too busy' scenarios. Making frequent back-ups is the single best thing to counter ransomware impact.

4. Our in-office Wi-Fi has no connection to our internal office network. Employees and visitors can freely use the Wi-Fi to connect to the Internet, but any attacks or security breeches experienced on the Wi-Fi won't impact ourbusiness processes or office Internet connections.

5. We use a secure third-party software library service to store and manage all the code we create for clients. This off-site storage controls access, provides version control (allowing us to return to an earlier version if needed), and is web-accessible from any computer.

While these actions don't eliminate the possibility of a ransomware attack, they will limit the damage and provide paths to rapid recovery from an attack.

We strongly encourage every organization to review its ransomware defenses and develop recovery scenarios. Contact us if you need assistance in this effort.

New PayPal Security Feature Can Result in Suspension of Your Site's Credit Card Processing

Carding, a type of fraudulent e-commerce activity, is now something PayPal is trying to detect and stop in its credit card processing service.

Carding is a form of credit card fraud where thieves sell stolen credit cards to other people. Because credit cards are often canceled quickly after being lost, a major part of carding involves testing the stolen card information to see if it still works before selling it. One way thieves test card information is by submitting purchase requests on the Internet. Several of our clients have experienced carding attacks like this in recent years.

PayPal credit card processing is now trying to detect carding and, if found, will suspend credit card processing on the offending site. The owner of the site will need to manually reactivate their PayPal account before card processing can resume. If you use PayPal for credit card processing, you should have already received an alert about this new feature directly from PayPal. If you haven't heard from PayPal, or want to know more about this change, click here .

Other News and Notes

Sporting a new name, vision, and mission, the **United Veterinary Services Association** launched their new web site this month.

The **American Feed Industry Association** 's new 2019 Liquid Feed Symposium micro-site launched with a fantastic new clickable expo floor plan . An admin panel allows AFIA staff to assign exhibitors to specific spots on the floor plan and for site visitors to see exactly where each exhibitor will be on the floor.

The **National Association of Senior Move Managers** recently archived its member listserv in favor of a new, interactive member engagement community. This new community allows NASMM members to share tips and tricks of the trade, as well as seek out services from other members. It's a great tool with lots of fun features.

The **Society for Laboratory Automation and Screening** launched its microsite in support of SLAS 2020 , 'Level Up Your Science', being held in San Diego in January, 2020. The site offers a wealth of information and services to conference attendees, exhibitors, sponsors, and the media that will be continually updated in the coming months.

Information about the 2019 Fall Conference of the **Pension Real Estate Association** is available in its new meeting micro-site.