frogworks

2023

Issue 10 Volume 13

Managing Your Technology So Your Business Doesn't Croak.

Ribb"IT" Review

INSIDE THIS ISSUE:

Protecting Your Business: Preventing and Detecting Ransomware Attacks:

Ransomware is malware that accesses your network and locks you out of your system. It steals important data and files, locks them, and demands payment in exchange. Preventing and detecting ransomware attacks protects your business, digital assets, and staff from these subtle threats.

Why Is it Important to Prevent and Detect Ransomware Attacks?

Once ransomware is on your business network, it is hard to get rid of. Prevention is a better plan. By preventing and detecting ransomware attacks, you protect:

- Company secrets and knowledge
- Employee and customer identities
- Financial information
- Other sensitive data

If your customers' private information gets out because of a ransomware attack, it could ruin the image of your business. Yet, this malware is getting harder to spot, so it's important to know how to protect your system from ransomware threats.

3 Ransomware Prevention Techniques

Cybersecurity teams should warn people in your network of digital threats. Your business information is kept safe by prevention plans.

(Cont next Pg)

This monthly publication provided courtesy of:
Alex Bleam,
Owner of Frogworks

Protecting Your Business: Preventing and Detecting Ransomware Attacks: (cont)

System Backups

You should keep your files and information in at least two places. Many people keep their files on their computer hard drives. But ransomware will pull documents directly from this location.

Use cloud solutions that are safe to back up your data. This works even better if the files are encrypted in the cloud.

Cybersecurity Measures

Set up security services that instantly put suspicious content in a separate area. This service should be available to all company machines. The quarantine measures will place emails and other messages with suspicious links or attachments in a secure area. You can then look at the suspicious content without risking your digital infrastructure.

Employee Education

The growing number of people who work from home has made ransomware attacks easier to do. When workers share files over networks that aren't protected, they unintentionally put their companies at risk.

Teach your employees how to share files safely and how to tell if an email might contain viruses.

Only let employees share files on private, safe networks. You can also try an email or knowledge base service that encrypts all data unless it is viewed by someone who can do so.

How to Find Ransomware Attacks

What happens when ransomware makes its way into your network? Below, you'll find the most common and reliable detection methods.

Signature-Based

A signature-based software compares a sample of malware code against code samples from familiar, internal files. It works well to mark malware that is already known. However, it won't recognize new ransomware that no one has seen.

Behavior-Based

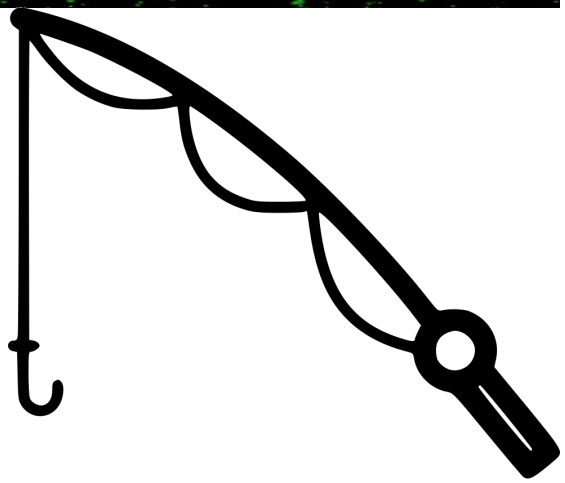
Behavior-based detection compares file behaviors rather than codes. It looks at the operating system's names, files, and strange behavior. It learns how older, harmless files react compared to newer ones to differentiate between trusted network traffic and attacks.

Deception-Based

Deception-based solutions lure ransomware. It creates false files as bait to trap ransomware. When ransomware attempts to encrypt a bait file, it reveals its intent to the solution. Deception-based software is among the most effective detection strategies.

You can't typically stop or mitigate an attack once it begins. You can, however, make detailed plans to stop and find ransomware attacks before they happen.

Staying Safe from Phishing Scams



Hackers steal personal information from people who are vulnerable by making fake websites and sending phishing emails. If you fall for a phishing scam, private information like your credit card number could fall into the wrong hands. You can protect yourself from hackers in several ways, which is good news.

How Do Hackers Scam People?

Hackers can send phishing emails to business employees when they get their email addresses. They do this to get the workers to give out personal information. Most of the time, hackers want money and will try to get the person they are communicating with to send them their credit card number or information about their bank.

If you fall for this scam, your sensitive information is at risk, and you need to move quickly to stop identity theft.

How To Protect Yourself From Phishing Scams

Phishing is one of the most common cyber attacks impacting businesses. In a phishing email, the hacker will pretend to be a trusted person, like a bank representative or fellow employee, to trick the receiver into sending sensitive information.

Use these tips to stay safe from phishing scams.

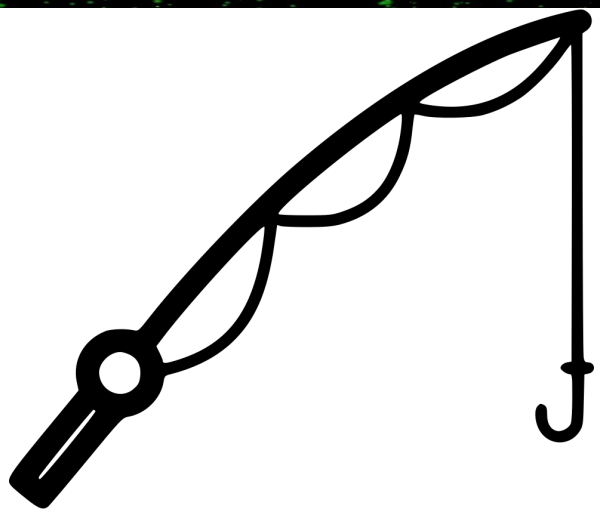
Recognize the Signs of a Phishing Email

Phishing emails are relatively easy to detect since most of them contain the same elements. Look out for any of the following items that are common in phishing emails:

- Unusual greetings
- Messages demanding urgent action
- Content featuring many typos and grammatical errors
- Strange senders asking you for login credentials or payment information
- Unknown attachments that use files like .zip, .scr, or .exe

If you receive an email that raises your suspicion, don't click on any links or open any attachments, as they may contain malware. Report the email to an IT professional who can mitigate the threat of further cyber attacks. (cont next pg)

Staying Safe from Phishing Scams (cont)



Set Up Email Filters

Your spam folder may automatically fill up with suspicious phishing emails, but savvy hackers are always looking to find ways to avoid the spam filter and get their emails to your inbox. You can set up additional email filters to protect you from scams, such as blocking the sender or flagging emails with strange attachments.

Perform Regular Data Backups

Protect your data by frequently backing it up to a hard drive or cloud service. If you access your business email on your phone, it's also wise to back up your mobile data. This ensures that you can access data even if your device is compromised.

Install Security Software

Boost your protection against phishing scams by using security or antivirus software that guards against hackers and cyber security threats. Make sure that you program automatic software updates so the program actively prevents new threats that may occur.

Use Multi-Factor Authentication

One of the best ways to protect your accounts from phishing scams is by setting up multi-factor authentication for your email account and any sensitive accounts, like your login to your banking website. You'll benefit from having additional security since your account will require another form of verification besides your password. This can be a one-time verification passcode, PIN, or correct answer to a security question.

We Have an E-Newsletter!!!

Do we have your e-mail address??? If you would like to receive our newsletter though email please visit us at:

www.getfrogworks.com/newsletter

Channel Futures. Leading Channel Partners Forward

NEXTGEN 101

MSP TO WATCH • 2021 WINNER