iTology

The Study of Your
Business I.T. Needs

Pandemic IT Security

Pitch Summary

Oklahoma businesses are at a greater risk of falling victim during this pandemic, and we would like your help to increase awareness.

There is an uptick in hacker activity that will likely lead to an increase in attacks during this pandemic. These attacks could cause small businesses who are already under distress to fail. We have tips for employers and employees to follow to help reduce the risk. We would like to get these tips out to the public to protect Oklahoma businesses from further harm during these difficult times.

Intro

Our small business community is in peril. Between COVID-19 and the decline of crude oil prices, every small business owner I have been in contact with is planning for the worst and hoping for the best.

How we (small business owners) handle this experience could mean the difference between closing our doors or surviving to fight another day. For the sake of our families and employees, we all want to survive to fight another day. We should all be more diligent than ever when it comes to cyber security right now. Both small business owners and our teams. Oklahoma's businesses' IT security is diminished during any significant event, especially a global pandemic.

Security Concern

Hackers, or malicious users seeking to cause us harm or to profit from us look for these opportunities to strike. We at iTology are seeing all the hallmark signs of a large-scale attack in the works.

Security Concern (continued)

We usually see two phases prior to a large-scale attack:

1) Seemingly useless attacks/compromises
2) Small scale attacks

Over the years, we have observed attackers evolve. They treat their efforts similarly to a legitimate business.

In the first phase they compromise email accounts, copy the victim’s contacts, and perpetrate their attack to those contacts. Often, these attacks seem harmless as there is no apparent damage done. In fact, they are spreading their reach by building their “marketing list.” This list is then used for their large-scale attack. The second phase is when they begin sending fraudulent emails to the accounts that they have already compromised in hopes that they are softer targets. These emails contain a payload that allows them to deploy their ransomware attack. As they fine tune their attacks to maximum their impact and profits, they launch into their large-scale attacks.

This is the phase that usually makes the news. Many businesses and municipalities across the country fall victim. If the victims do not have the appropriate security measures in place, they are left with two choices; lose their data or pay the ransom and hope they decrypt their data as promised.

This time, the attackers are adding an additional threat. They are not only encrypting the data and requesting payment to decrypt the data. They are also threatening to release the data they have stolen into the public domain if they are not paid. This threat can be especially damaging depending on the type of business and the nature of the data.

Timing

There are two key factors that make us more vulnerable than usual:

1) Distractions
2) Change of daily habits/behaviors

Similarly, to distracted driving it can also be dangerous to be distracted when performing your daily work tasks. The impact is financially dangerous vs physically dangerous. It's nearly impossible for us to not be distracted with all the changes and information we are receiving in the work place during this epidemic.

Imagine, an email comes in from someone you know (who has been compromised) and you click on an attachment without thinking. It takes you to a legitimate looking website that requests your email credentials to access the document your contact sent you. You enter your credentials, and your account is compromised.

Most of us have our daily routines. We get up in the morning, we get dressed, we grab a bite to eat, we grab our keys, our wallets or purses, and our phones. But when we stay somewhere like maybe a hotel in another city, our routine is thrown off and the likelihood of leaving something in the hotel is increased. That is why many of us pay close attention and are extra diligent about not leaving something in the hotel when we checkout.

The same applies to our daily work lives. Right now, with more and more people working remote, our daily routines are uprooted. And in this case, we don't know what to be extra diligent about. We're figuring out our new daily routine as we go. And when you introduce children staying home from school to the mix, it only adds more opportunity for the attackers to prey on us.

Summary

Given all of this, it would be easy for someone to be overwhelmed. We (IT Providers) are here to help. Don't Panic, Plan!

In the event your business is impacted by ransomware, FBI instructions on reporting the incident can be found at: https://www.ic3.gov/media/2016/160915.aspx

Here are some tips to help keep you and your employer or employees safe. We are all in this together.

Employer Tips

- Partner with an IT Provider
- Use business class e-mail
- Enforce Multi-Factor Authentication (MFA)
- Use Secure Remote Access
- Disable accounts with the username admin or administrator
- Train your team

Employee Tips

- STOP! THINK! VERIFY!
- Verify e-mail attachments before opening
- Verify hyperlinks before opening
- Report anything suspicious to your management or IT Provider
- Verify the website's URL before entering a password
- Use a password manager
- Don't save passwords in your browser

Thank you for your consideration,
Cory Carson
Chief iTologist
iTology
CoryCarson@iTologyOK.com