You can find the NIST Ransomware video and other SBCC videos at:
https://www.nist.gov/itl/smallbusinesscyber/videos

Ransomware

What could be more terrifying to you, a small business owner, than to discover you are locked out of your own computers because you've been hit with ransomware.

What is "Ransomware"?

Ransomware is a type of malicious attack where attackers encrypt an organization's data and demand payment to restore access.

Here's an example of how a ransomware attack can occur:

1. A user is tricked into clicking on a malicious link that downloads a file from an external website.
2. The user executes the file, not knowing that the file is ransomware.
3. The ransomware takes advantage of vulnerabilities in the user's computer and other computers to propagate throughout the organization.
4. The ransomware simultaneously encrypts files on all the computers, then displays messages on their screens demanding payment in exchange for decrypting the files.

Common ways ransomware can hit you:

- Email – phishing emails can trick you into clicking on an attachment ("Urgent Invoice") that allows the malicious software program to take over your computer.
- Malware – if your network or software is vulnerable, a cybercriminal can sneak in and plant malicious code. It might sit unnoticed for a period of time, allowing the bad guys time to access files and steal data, then finishing up with unleashing ransomware so you can't see the damage.

Ransomware is a common threat against any business, large or small. It can put a company out of business or disrupt operations for a long period of time. Paying the ransom can be very expensive and there's no guarantee that data will ever be recovered. If customer data is stolen, it may trigger state data breach notification laws.

Ransomware disrupts or halts an organization's operations and poses a dilemma for management: does the organization pay the ransom and hope that the attackers keep their word about restoring access, or does the organization not pay the ransom and restore operations themselves?

Fortunately, organizations can take steps to prepare for ransomware attacks. This includes protecting data and devices from ransomware and being ready to respond to any ransomware attacks that succeed.

Don't assume your business is too small to get hit. The nature of ransomware is that the cybercriminals work to ensure their malware spreads as widely as possible, infecting the computers of individuals and businesses of all sizes.

TIPS & TACTICS RANSOMWARE

NIST CYBER

Quick steps you can take *now* to PROTECT yourself from the threat of ransomware:

1 USE ANTIVIRUS SOFTWARE AT ALL TIMES

Set your software to automatically scan emails and flash drives.

2 KEEP YOUR COMPUTER FULLY PATCHED

Run scheduled checks to keep everything up-to-date.

3 BLOCK ACCESS TO RANSOMWARE SITES

Use security products or services that block access to known ransomware sites.

4 ALLOW ONLY AUTHORIZED APPS

Configure operating systems or use third party software to allow only authorized applications on computers.

5 RESTRICT PERSONALLY-OWNED DEVICES

Organizations should restrict or prohibit access to official networks from personally-owned devices.

6 USE STANDARD USER ACCOUNTS

Use standard user accounts vs. accounts with administrative privileges whenever possible.

7 AVOID USING PERSONAL APPS

Avoid using personal applications and websites – like email, chat, and social media – from work computers.

8 BEWARE OF UNKNOWN SOURCES

Don't open files or click on links from unknown sources unless you first run an antivirus scan or look at links carefully.

Steps you can take *now* to help you RECOVER from a *future* ransomware attack:

1 MAKE AN INCIDENT RECOVERY PLAN

Develop and implement an incident recovery plan with defined roles and strategies for decision making.

2 BACKUP & RESTORE

Carefully plan, implement, and test a data backup and restoration strategy – and secure and isolate backups of important data.

3 KEEP YOUR CONTACTS

Maintain an up-to-date list of internal and external contacts for ransomware attacks, including law enforcement.

NCCoE
NATIONAL CYBERSECURITY CENTER OF EXCELLENCE