Cyber Security Checklist

How to Protect Your Business from Cybercrime!

Step 1
Patching

Patching is a piece of software that updates the various systems and programs and their supporting data. It is a key element to protecting yourself from outside intrusions by fixing security vulnerabilities and other bugs.

Your best bet is to set these on auto-updates, let them update without thinking about it.

- **Operating System**

- **3rd Party Applications** - don't ignore these updates when they appear
  - ›Adobe
  - ›Quicken Books
  - ›Flash
  - ›Java

- **Firmware** - these are your front-facing pieces of hardware that contain software
  - ›Network Drives
  - ›Switches
  - ›Routers

www.us-cert.gov
Want to get notification on the latest threats circulating and which updates are available?
Visit www.us-cert.gov (United States Computer Emergency Readiness Team) and sign up for release notifications. It's a lot of information, but the more you read, the more aware you will become of the threats that surround us and how to do your best to prevent them.

CONNECTICUT
COMMUNITY BANK, N.A.®

Step 2
Firewalls

Firewalls are security systems that monitor and control the incoming traffic based on security rules you have pre-determined are best for your company. They establish a barrier between your internal network and threat from outside networks.

Remember, it's not enough to purchase and install the firewall, turn on all the functions made available.

- Gateway anti-virus - anti-virus security that checks incoming traffic for viruses and blocks potential threats before they reach your network.
- Content filters - program to screen and exclude from access or availability Web pages or on subjects that are deemed unacceptable for your business.
- GOipfiltering - allow you to block connections coming from a specific geographic location.
- Messaging Gateway - help prevent maleware, SPAM and emerging threats from entering your email system.

Step 3
Recovery

You can purchase and have back-up files for all your systems and data. But guess what, the recovery of these is only as good as your back-up system and your ability to restore!

- Invest in a good back-up system.
- Test the system once a year.
- Create a detailed Disaster Recovery Plan - layout the who, what, where, when and how.
- Create an Incident Response Plan - know your immediate steps to do when you get hit.

Step 4
PEBKAC

Problem **E**xists **B**etween **K**eyboard **A**nd **C**hair! It's important that your employees pay attention to threats that they receive directly in their everyday emails.

Cyber criminals have become very adept in spoofing emails that look like they are from legitimate companies such as FedEx and Amazon. Even those from a trusted source, such as a CEO, CFO or HR Director can be spoofed and contain links with malicious code embedded in them.

Emails are also surfacing that spoof a company president or CFO with requests that money be wired out to pay a vendor or customer or to move funds.

Step 5
SAR

Stop - Assess - Report! Train your employees to take a look at the emails they are receiving.

Stop - don't open suspicious emails or click on any links.
Assess - would my CEO request this information in an email? Why would FedEx be sending this to work?
Report - talk with your co-worker or manager about it.

SAR - Create reminders and place these letters everywhere in your office!

CONNECTICUT
COMMUNITY BANK, N.A.®

Online Security Practices

While no tools or automated software is 100% effective, the best solutions to protect your business are to be well informed and use common sense. Using a multiple vendor, multi-layer approach to system design can significantly reduce your chances of being a victim of cybercrime. To assess the risks associated with a cyber-intrusion of your business' online systems and critical client data, ask yourself the following questions:

1. Does your business have a hardware based firewall at the network level?
2. Does the network firewall include anti-virus, anti-spyware and anti-spam services along content filtering and intrusion prevention, detection and real-time reporting?
3. At the individual PC level, does each computer have centrally updated and monitored anti-virus, anti-spyware and anti-spam software loaded?
4. Are your computers set up to automatically update your operating system and applications for the latest available security and critical updates?
5. Do you consider your browser security setting to determine how much or how little information the browser can accept from, or transmit to, a website?
6. Does your business have a security policy in place that includes such policies as disaster recovery, use/storage of passwords, use of social media on work computers, etc.?
7. Does your business back-up critical files in case of an issue that disables your systems?
8. Has your business identified an individual to review security policies and practices on an ongoing basis?
9. Are you aware of the laws governing the protection of personal information in your state?
10. Do you have cybercrime insurance to protect your data and liability exposure in the event of an intrusion?
11. Does your business have a training program to educate employees on best practices to avoid becoming a victim?

These are just some of the basic steps a business can implement to assess and protect itself from cybercrime. Your business should have a network security assessment and review conducted by a certified information technology firm that specializes in network security. This evaluation will help you to identify the "next steps' in securing your network and date from unauthorized access and distribution.

This information is intended to provide guidance on this important topic. Specific questions regarding the safeguards of your organization's computer networks should be directed to your IT Manager/Director.

DARIEN
BANK & TRUST®
A Division of Connecticut Community Bank, N.A.®

THE
GREENWICH
BANK & TRUST COMPANY®
A Division of Connecticut Community Bank, N.A.®

NORWALK
BANK & TRUST®
A Division of Connecticut Community Bank, N.A.®

STAMFORD
BANK & TRUST®
A Division of Connecticut Community Bank, N.A.®

WESTPORT
NATIONAL BANK®
A Division of Connecticut Community Bank, N.A.®

CONNECTICUT
COMMUNITY BANK, N.A.®

EQUAL HOUSING LENDER
Member FDIC