



Cybersecurity Tips for **Business**



Protect Your BUSINESS

Running a small or medium business—you are likely very busy and wearing many hats. Reducing your company's risk is key to your success. Processes and procedures relating to cybersecurity are a must and begin by educating your staff on best practices.



Protect Your COMPUTER

Technology can be used to keep your computer and digital devices more secure if you remember to keep your software and firmware up to date. Remember, STOP. THINK. CONNECT.™ before you take any actions online.

DEVELOP A SECURITY AND PRIVACY POLICY

Instruct your employees on how to protect your corporate and customer information. Explain to your customers how you will keep their personal data private and include the following for your staff:

- Ensure all employees understand the policy and penalty for violations
- Restrict peer-to-peer file sharing, personal storage media and user software
- When in public, stay private. Never use public computers, such as those in libraries or Internet cafes, for online purchases or banking. Stick to e-mail or general Web surfing on those computers
- Establish personal use policies for email and the Internet, blogging, and excessive use

PROTECT YOURSELF AND YOUR CUSTOMERS FROM IDENTITY THEFT

Handle credit/debit card and other personal information securely. Do not store this information without appropriately securing it.

SECURE YOUR MOBILE DEVICES AT ALL TIMES

Laptop and all digital device theft is a growing threat to your business information. Physically secure these systems

and consider encrypting sensitive data. Ensure you have a comprehensive cybersecurity policy in place for best practices especially if you have a Bring Your Own Device (BYOD) practice in-house.

RAISE YOUR STAFF AND CUSTOMERS' AWARENESS ON CYBERSECURITY BEST PRACTICES

Schedule a workshop for your staff and customers on the best cybersecurity practices and help them learn about pitfalls to avoid. Request a Securing Our eCity foundational workshop.

ESTABLISH A SOCIAL MEDIA POLICY FOR YOUR ORGANIZATION

Social media is an excellent method of reaching potential customers. However, it is also a known haven for malware. Be certain you have a social media use policy in place for all employees, unless they are part of your corporate social media team.

KNOW WHO TO CONTACT

Know who to contact if you believe your organization has been breached. Tips and suggestions can be found on the Securing Our eCity website.

USE AN INTERNET FIREWALL AT ALL TIMES

The firewall is your first line of defense in protecting your computer, because it helps to obscure your computer to online attackers and many types of malicious software.

KEEP YOUR OPERATING SYSTEM UP TO DATE, ENABLE ITS AUTOMATIC UPDATE FEATURES

Online criminals are constantly at work devising new ways to attack your computer and invade your privacy. Fortunately, software companies work even harder to counter those threats and to provide you with updated tools that you can use to protect your computer.

INSTALL AND MAINTAIN ANTIVIRUS AND ANTISPYWARE SOFTWARE

Antivirus and antispyware software helps to protect your computer by scanning e-mail, applications and data that resides on your computer. Strong antivirus and spyware programs can detect and remove viruses and spyware before they have a chance to damage your devices.

ESTABLISH A POLICY FOR USE OF PUBLIC WI-FI NETWORKS

While convenient, public Wi-Fi networks can potentially expose proprietary intellectual property if used while conducting business. You may want to consider providing your staff with Virtual Private Network (VPN) access or look for Wi-Fi encryption applications.

CHOOSING YOUR PASSWORD

Perhaps one of the easiest, yet most challenging security measures that can be implemented is the regular updating of one's passwords. The objective is to remember it without writing it on a post-it that you keep next to your computer, but also making it complex enough that it is not easy for hackers to gain access to your computer. Avoid some of the following pitfalls and consider a "pass-phrase" like "mybirthdayis1970Jan15."

The top ten things to avoid include:

1. Any part of your name
2. Your account name or numbers
3. Anything less than 7 characters long (*system permitting*)
4. Any part of the name of a member of your extended family (*including pets*) or, worse, a colleague
5. Name of your computer's operating system
6. Significant numbers (*phone number, car license number*)
7. Names of locations or points of interest
8. Favorite or most-hated things
9. Easy associations with favorite or most-hated things. (*for instance "Swan_Lake" is a bad password for a ballet freak*)
10. Popular choices such as "wizard", "password", "today", "AAAAAAA", "QWERTYUIOP", etc.



www.securingoureconomy.org

The Securing Our eCity® Foundation
is helping to make a cyber-safe environment
where we can live, work and play
through cybersecurity
awareness, education and preparation.

This piece is sponsored by ESET® North America and San Diego Gas & Electric



STOP | THINK | CONNECT™