Common Cybercrime Types and Preventative Measures You Can Take Today

When is the last time you've gone 24 hours without touching your phone? How about without using a computer?

Today, dinner reservations can be made online. Gifts can be bought and shipped. We even talk to our friends using apps. Technology surrounds us… we're constantly immersed within it. However, despite our unique usernames and passwords, internet security is not bulletproof.

1. Theft of Sensitive Information or Intellectual Property

2. Hacking & Corporate Account Takeovers

3. Malicious Files and Software

3 Common Cybercrime Activities

Here's a quick list of the most common cybercrime types:

1. **Theft of Sensitive Information or Intellectual Property**

   Most people associate this with identity theft; however, for businesses it can mean theft of sensitive information or even intellectual property. Employment records, customer data, and confidential company documents - they can all be stolen and used by cybercriminals.

   South Carolina's Department of Revenue experienced this in 2012, when cybercriminals broke into their computer systems and stole 3.6 million Social Security numbers and 387,000 credit/debit card numbers. On top of that, the break began in late August and wasn't discovered until October by the U.S. Secret Service.

2. Hacking & Corporate Account Takeovers

Hacking involves accessing a person's (or business') information illegally. This can be done through email accounts, social media pages, and company websites. One form of hacking is Corporate Account Takeovers, which can be damaging to many businesses. It usually entails cybercriminals stealthily obtaining financial banking credentials to a company. They then hack one of the company's computers remotely and begin to steal funds from your bank account

3. Malicious Files and Software

Viruses and malware are commonplace on the internet. Oftentimes, it starts with a prompt on a website or within an email to employees asking them to visit a link and complete an action to gain access. Once they have access, they will infiltrate the network and steal valuable information.

Despite our unique usernames and passwords, internet security is not bulletproof.

Preventative Measures You Can Take

The first and easiest way to protect yourself from cybercrime is to protect your computers. Install anti-virus software and keep it updated. Also, make sure you install a firewall and keep your operating system updated.

Another measure you can take is to become security conscious. Email scams and frauds are regularly used to attack people, and you'll be surprised how many fall for their tactics. By becoming more aware and cautious about suspicious emails and links, you can help prevent hacks.

It also helps to be ready for a security intrusion as they frequently happen, despite defensive measures. IT professionals recommend having a plan in place to address an attack if it does happen. Make sure sensitive information is restricted to key individuals. For businesses, it's not a bad idea to also have business insurance to help recover financial losses due to cybercriminals.

If you need more help, hire a security expert to examine any vulnerability you might have and recommend changes to secure vital information.

Berkley Industrial Comp is pleased to share this material with its customers. Please note, however, that nothing in this document should be construed as legal advice or the provision of professional consulting services. This material is for general informational purposes only, and while reasonable care has been utilized in compiling this information, no warranty or representation is made as to accuracy or completeness.

Berkley INDUSTRIALCOMP | a Berkley Company