Blog for MPA Networks

https://www.mpa.com/blog.aspx?p=tis-season-small-business-cybercrime-heres-protect-company

'Tis the Season—for Small Business Cybercrime. Here's How to Protect Your Company

Posted January 7, 2015

The holiday season means more than shopping and gift giving. It also now marks prime season for cybercriminals and hackers around the world — and they're coming after small businesses in the U.S.

"Targeting" Target—via Small Businesses

You may have seen a segment on the November 30 broadcast of *60 Minutes* which looked at today's record levels of data security breaches among large national retailers. They spotlighted the credit card nightmare at Target stores, which occurred a little over a year ago.

It's now known that sophisticated hackers in Eastern Europe pulled off that massive caper not by directly "targeting" Target, but by seeking out smaller vendors who were doing business electronically with the company. They finally found a small HVAC contractor in Pennsylvania who had been performing work in nearby Target locations. Bypassing comparatively weaker IT security, the hackers located the contractor's sign-in credentials for Target's vendor interface. Once inside the Target network, they unleashed viral malware which attached itself to point-of-sale terminals in Target stores coast-to-coast. The result: roughly 40 million American consumer credit card numbers (including yours?) were suddenly up for grabs on the international black market.

Enabling a nationwide consumer panic is not how any small business wants to be remembered.

The holidays, and the post-holiday sales season, are particularly attractive to the cyber underworld because of the higher volume of commercial activity across our modern digital economy. And they know hacking into a Fortune 500 company — with vast security resources — is about as promising as trying to hop the fence at Fort Knox. They'd rather look for smaller companies with vulnerable security flaws, such as weak data protection policies, obsolete or unpatched security software, or careless employees.

The consequences hackers can inflict on a small company can range from compromised customer records to virtual extortion through "ransomware" and outright theft of cash. And unlike the generous fraud protections offered to those credit card customers at Target, unauthorized withdrawals from a commercial account may take weeks to resolve — or longer, pending investigations by banks and law enforcement. And unlike credit card fraud, in many cases you may never get your money back!

Now is an excellent time to review your company's defenses against hacking and cybercrime.

Start with the Basics

Remind your employees to choose difficult company passwords (and periodically change them). Better yet, have your administrator set your password policy to require changes once a quarter or even once a month. Yes, users don't like it — and yes, your security will improve and your business will be protecting itself.

Have your employees remain on the lookout for phishing emails — particularly "spoof" emails made to resemble notices from trusted websites like Amazon, Facebook, or your bank. One click on a phony link can quickly spread malware throughout your company and disrupt your business fast. To educate your employees, you might have them read this.

One malicious email could cost you thousands of dollars. Get the facts. Here's how to identify a malicious email.

If your employees think they're good at picking out a malicious email vs. a real one, have them take this quiz. And even if they *don't* think they're good, have them take the quiz anyway. Then have them review the quiz answers. Your employees may be surprised. (Hint: we've been told this quiz is a good educational tool — and can save frustration, money, and downtime.)

Security, and Then Some

Talk to your IT service folks and make sure your workstations, laptops, and any servers you might have in your office or in the Cloud are continually being patched for security flaws, and that your anti-virus systems are being constantly updated (as often as multiple times a day is recommended).

Next, consider a comprehensive security audit to identify likely weaknesses a hacker could exploit. Then patch those holes with state-of-the-art IT safeguards, including the latest enterprise-grade malware protection suites, hosted email security, extended encryption for Cloud applications, and optimal firewalls.

Cybercrime is out there, and growing by the day. To learn even more about precautions you can take against these threats, click here.