Keep Your Organization Out of the News

We frequently hear about yet another data breach that has occurred or that more sensitive data has been found publicly online or for sale on the dark web. Companies and businesses need a greater focus on what can be done to protect organizations and individuals from this type of cybercrime.

Thieves are after all types of information. Often it's called "confidential" or "sensitive." Both categories are valuable to identity thieves and those wishing to capitalize from you or your organization. The list of information that is valuable can get lengthy, but here are some items that are most common and most valuable:

- Names
- Addresses, physical and email
- Social security numbers
- Financial accounts and other related data
- Debit and credit card numbers
- Online login credentials for any account
- Security questions and answers
- Birth dates
- Driver's license numbers

What can you do to prevent information theft?

While this list can also get long, let's start with these items:

- **Create policies** and processes regarding performing financial transactions and proper data handling.
- **Train employees** on security and how to form and maintain safe data handling habits. Train them about phishing, strong passwords, and the importance of following procedures when it comes to financial transactions and data handling.
- **Require your vendors** and contractors to abide by your policies and include penalties for non-compliance.
- **Enforce your policies**.
- Minimize what is posted on **social media**. You may not think there is harm in advertising your job title on social media, or other sites, but spear-phishers use that information to do a variety of things such as business email compromise (BEC). The FBI warned that the dollar figure in losses due to this type of fraud surpassed the $3.1 billion over the last three years!
- Create and perform an **annual review** of your security and security response plan. Make adjustments as needed.
- Create a **patching schedule** and plan so that all systems can be kept up to date.
- Ensure that all systems in your organization have **anti-malware software** and that it is kept updated.

The cyber criminals use a variety of methods to get into a network and they don't necessarily limit themselves to one way at any given time. They often combine phishing with malware attacks, or online advertising with malware called 'malvertising.' In addition, ransomware and scareware are also lucrative methods for hackers to get information and money from victims. However, do not pay to get data back. Instead, put a good backup process in place so you can restore from a recent backup, should ransomware strike.

Don't forget that accidental release of information is also a way that data gets into the wrong hands. Lost and stolen laptops and portable drives are one way. A few years ago a field was littered with sensitive and confidential information on dental patients with no real explanation as to how it got there. Not so long ago, medical records from a radiology center were found scattered along a freeway when a waste disposal company did not properly follow processes for caring for the documents.

Even simple mistakes such as a typo in a web address can lead to a serious data breach. Take time to make sure your organization is not the next one putting others' information at risk for identity theft and making headlines.

Get the lastest information from our website. Scan the QR Code to go directly to this page.