Lower Your Risk of Business Fraud

For those responsible for the security of the corporate network, or even a small business network, it's important to take a layered approach to securing the information that resides on and passes through it. It the industry, it is generally assumed that **at least five key layers of protection** are necessary for doing this.

- **Secure your email gateway.** It is no surprise that most of the breaches that occur start with email. Typically it's a phishing attempt, including the more targeted versions of spear-phishing and whaling. Usually a message is sent with a link or attachment that will spew all kinds of doom if it's clicked or opened. Therefore, make sure you have some level of protection to prevent as much of this as possible. It can be an appliance, a cloud solution, or whatever your security strategy and budget will allow.
- **Use a DNS protection tool.** Every time a user clicks a link, it must go through a Domain Name System (DNS) server. Using this gives an extra layer of safety at a relatively low cost.
- **Implement endpoint protection.** This could be multi-factor authentication tools, anti-malware software, or Virtual Private Networks (VPNs) for those who work remotely. Bank of Utah offers fraud protection services to customers by allowing them to monitoring check payments and by triggering an actionable alert when an ACH debit hits your account to approve (or not approve) the expense.
- **Pay attention to user behavior.** Use analytics tools and watch for trends. If something is out of the ordinary, you can react to it faster. For example, if Bob was downloading ten files per day, but suddenly you notice it jumped to a hundred or even a thousand, take a closer look. It could be a very busy day for Bob, or it is more likely something nefarious.
- **Train users and test their knowledge.** It doesn't do much good to train someone if you never really know if it works. Phishing is by far the primary way malware enters a network, so make sure your users are trained on what it is, what it can do, and how to identify and avoid succumbing to it.
- **Ensure good policies and a security response strategy.** Review it and update it at least annually. Don't forget to enforce the policies for everyone that connects to your network.

Ultimately, you can never be 100% safe. But the more you know, the more you can implement good security practices; and the more your users know, the less risk it is to the organization.

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