NEBRASKA BROADBAND

www.broadband.nebraska.gov

MAKING SECURITY A PRIORITY

Security of systems, information and data are all critical to the success of small businesses – and safety of individuals. New devices and applications mean more focus and options on your information security.

NEBRASKA BROADBAND INITIATIVE

The Nebraska Broadband Initiative proudly shares information to support the increased adoption and use of Broadband high speed Internet.

To provide a better understanding of making Security a Priority, University of Nebraska - Lincoln technical experts and successful small business leaders explain the importance of security for systems, information and data.

To learn more about computer security, watch the webinar with UNL experts and small business leaders at:

http://broadband.nebraska.gov/events

Presented by Ed Media and Nebraska Broadband Initiative
UNL Planning Team

AIM Institute

Nebraska Information Technology Commission

Nebraska Department of Economic Development

Nebraska Public Service Commission

University of Nebraska–Lincoln

The Broadband Mapping and Planning Initiative is funded through a grant to the Nebraska Public Service Commission by the U.S. Department of Commerce's National Telecommunications and Information Administration and aims to increase broadband adoption and utilization. Project partners include Nebraska Public Service Commission, University of Nebraska–Lincoln, Nebraska Information Technology Commission, Nebraska Department of Economic Development and AIM Institute

MAKING SECURITY A PRIORITY

Why is Security Important?

For businesses, especially small businesses, security can often be a huge challenge. With minimal, or in some cases zero, IT staffing important security considerations can be overlooked. Businesses need to have a security policy in place, make sure that online transactions are carried over secure channels, and be aware of progress in the security arena.

"You can build the best safe in the world, but if you leave the keys lying around on the coatrack, the safe is not going to help you secure your documents or your jewelry. In the same way, you could have a very secure computer, but if users aren't knowledgeable about security, the system becomes vulnerable." (Byrav Ramamurthy, UNL Computer Science Professor, specializing in high-speed network and network security)

Creating Secure Passwords

- We often hear that we should use secure passwords, cut we don't think about why. The "why" is actually very important.
- People think that nobody will guess their password, but really password attacks are sophisticated. They are clustered, automated and done by machines. It's not just a single individual guessing.
- Compromising a password and account gives a hacker a resource. They may not be after you specifically, just after the resource. That's motivation enough.

Ensuring Payment Processing Security

- When buying or selling products online, verify that you see the lock symbol and HTTPS in your browser to confirm the transaction is encrypted.
- Always verify that your payment processing vendor has up-to-date security certificates, including SSL (Secure Sockets Layer) and is PCI (Payment Card Industry Data Security Standard) compliant.

Outsourcing Security

- Third-party online vendors like eBay, Amazon, Esty and Grow Nebraska not only offer a great base of customers to market your products, but also take care of securely processing payment transaction and safely storing customer data.
- Other third party vendors like PayPal and Shopify allow you to sell from your website while handling secure payment processing externally from your website.

"We knew eBay would be part of our selling mix, and it went so well that we just stayed with it. We realized the power of their security and marketing. It's a great marketplace and a trusted place to do business. We don't have to handle credit card information or other aspects of the business end. It takes those decisions out of our hands." (Kelly Neill, president and co-owner of Billiard Buyers Group)

Choosing an Outside IT Company

- Understand what type of security they provide
- Ask for sample reports of their work
- Get referrals
- Ask about compliance for customer data and adherence to industry standards (COBIT, SAS 70, PCI, SOX, HIPAA)
- Beware of "snake oil" false claims. Good security should be built into a product, not constantly upsold or made too complicated
- Make sure you have good rapport with the employees.

"Bouncing back from being hacked would not only be hard technically, but it would be difficult to rebuild your customers' trust. It's tough to tell customers that their information has been compromised. It would take time, energy and money to rebuild your reputation." (Kelly Neill)

Understanding Types of Security

External Security

- Network security
- Data Security
- Physical Security
- Vendor Security

Internal Security

- Restricted access
- Policies and procedures

Developing a Security Plan

Know the value of your data

- Low: General company information, company address, phone numbers, email addresses, etc.
- Medium: Business processes and procedures, business reports, work product, etc.
- High: Customer data, including, but not limited to credit card information, addresses, bank information, etc.

Mitigate your risk for a security breach

- Promote employee awareness
- Make sure your perimeter is secure
- Have policies and procedures in place as to what is allowed on the network
- Make sure policies are up-to-date and that employees follow them consistently

"Security has changed in the past few years with the advent of mobile devices. The need to protect the network has moved away from the local office to the coffee shops. We need to figure out how best to extend the security for our networks to wherever this device may go." (Chris Hobbs, Information Security Officer for the State of Nebraska)