

CONNECTED



AN ELECTRONIC REPORT FROM THE CUNA TECHNOLOGY COUNCIL

Colorado Springs Summit A Smashing Success!

The fifth annual CUNA Council Technology Summit concluded August 12 to overwhelming enthusiasm from conference participants. "The conference and the Council provide an excellent opportunity to network with credit union technology peers," said one attendee. The CTC

executive committee would like to offer a special thanks to the conference committee led by Dan Kinne, Silver State Schools FCU, Las Vegas, NV for all of their hard work and commitment to making the conference a success.

Nestled at the foothills of the Rockies, the Colorado Springs Wyndham Hotel was the location for this year's Summit. With an emphasis on Internet commerce and electronic information and delivery, attendees were able to immerse themselves in a technologically advanced environment.



After two days of conference sessions, it was time to unwind with an outing to the Flying W Ranch. Networking among the technology gurus was very apparent and a good time was had by all. It was truly a unique Colorado experience.

Don't forget to plan for next year! The sixth annual CTC Summit will commence August 15, 2001 at the Wyndham Palace Resort and Spa in Lake Buena Vista, Florida. Make plans now to attend. You may want to consider making this your family's summer vacation and enjoy all Disney World has to offer. Special conference pricing will be available for Disney World tickets. Plans are already in motion for the conference agenda for next year and you won't want to miss it. ♦

CTC Developing a Web Subcommittee

A new subcommittee, led by executive committee member John Bock, Community CU, Plano, TX has been formed to assist in the development and chart the direction of the CTC Web site. As many of you know, the CTC Web site will have a new look and feel in the near future. This subcommittee is being created to assist with our continuing efforts to offer the majority of CTC benefits online. If you are interested in serving on this committee, please contact John at Jbock@communitycredit.org.

Volunteers Needed

If you have an interest in serving on other CTC subcommittees, we are always looking for volunteers. Subcommittees include communications, membership, conference and education. If you did not have a chance to sign up for one of these at the recent conference, you can still do so by contacting Mike Pytlik at mikep@commfamily.org. Mike will put you in touch with the executive committee member chairing that subcommittee.

Convergence

By Alan Darbe, State Employees Credit Union, Lansing, MI

Convergence is the new buzzword in the voice and data communications. Briefly, it means that voice and data technologies are growing together. In the recent past the terms Voice over IP or VoIP have been used to describe this event.

When you think about it, convergence has been in place for many years. The difference is that it is reversed data over voice. A modem by its very definition is IPoV or IP over Voice. Modems provided the means for connecting computers to one another using voice lines. As time has passed, the quality of telecom equipment has greatly improved, dedicated lines eliminated the need for modems, and network interface cards were used to replace them. Before voice was even available, data was transmitted using the pseudo binary Morse code.

How will convergence affect the work we have to do in managing our voice and data networks? In time, it should ease the need for two disparate but fundamentally the same networks. Everyone with a PC has a telephone and nearly everyone with a telephone has a PC. Where the specific needs of the voice network will appear is in "quality of service" or QOS. At lower network speeds, the packet needs of a voice network are higher than that of a comparable data network. The human ear cannot "queue" packets. New hubs, routers and switches will need to have a QOS ability.

Many of them already have the ability to give priority to specific network traffic.

How will this help us? Lucent Technology is currently testing their new IP telephones, the Lucent Definity telephone system (PBX*) which is already capable of being on the data network. These telephones contain a two port hub. This will allow the telephone to be attached to the network and the individuals PC. This results in a single wire to the workstation containing both voice and data. This will eventually reduce the wiring and maintenance costs to the organization.

Another area for convergence to help us beleaguered IS - Telecomm types, is the ability to place ISDN connections in the PBX and have the PBX send the call to the network. Many of us use ISDN service on our PBX systems to provide caller id and other services from the telephone company. This means you may be able to provide ISDN dial-up services to staff and members for a minimal cost.

As with any developing technology, the key is to have good information. Talk to your PBX provider or local telephone company for more information. ♦

**PBX - Private Branch Exchange. The telephone system at a customer's location that connects to the telephone company and routes calls to the appropriate internal number.*

Securing Your Web Site

By Darryl Mataya, Vice President, Cyberspace Financial Services (www.cyfi.com), Madison, Wisconsin

Internet security is an interesting topic. Everybody loves to write and talk about it, but nobody really knows what is going on. That's because we talk about security in the abstract. Those who have secure systems that have not been breached or invaded know it. Those people rarely talk about it. Those who have been attacked won't talk about it unless they have to - fearing that knowledge of an attack would be bad publicity. This year's well publicized attacks against major e-commerce sites like eTrade, eBay and Yahoo demonstrate that perhaps this is changing. It is probably better for the entire Internet community if we stop the practice of pretending it only happens to

the "other guy". These threats are real, they happen to all of us, but there are a large number of remedies that protect you from loss or catastrophe.

Securing your web site can be quite simple, or somewhat complex. It depends on what your site does, where it is hosted, and what mechanisms are in place to protect it. First we need to identify all the threats faced by a typical financial institution web site. Then we will identify the things we do at CyFi for our clients to help protect against those threats.

We sort out the various threats to web sites by putting them in the following eight categories:

1. The site is not available. Perhaps the most obvious “threat” to a web site’s well being is that it simply must be available. Sites that are unavailable a high percentage of the time or do not seem to work properly (e.g. have many “broken” links and non-working features) give a visitor the sense that the institution behind the site is not knowledgeable or serious about its operation. From that standpoint, unavailable sites simply reflect poorly on the institution’s operations and choices.

2. A site gets wiped out. Another obvious issue with web sites is protecting them from being deleted or lost in some other disaster. In this case, we are basically concerned with being able to restore all of the physical files and resources necessary to make a site operational.

3. A site is vandalized. There have been a number of highly publicized cases where vandals obtain access to a web site and then modify it—often in a non-complimentary fashion! This usually occurs as a result of a web access password being compromised or stolen. In this scenario, it is also fairly easy for the vandal to delete the entire visible site and/or create links to offensive or competitive sites. A big concern in this scenario is the damage such an event can do to the institution’s goodwill—something that can be difficult to replace.

4. Unauthorized access. Web sites can hold some member and prospect information, or, more importantly, act as a gateway to Internet banking systems where the threat of damage via unauthorized transactions can be high. This threat refers to the fairly obvious situation where someone unauthorized to view this information gets access to it.

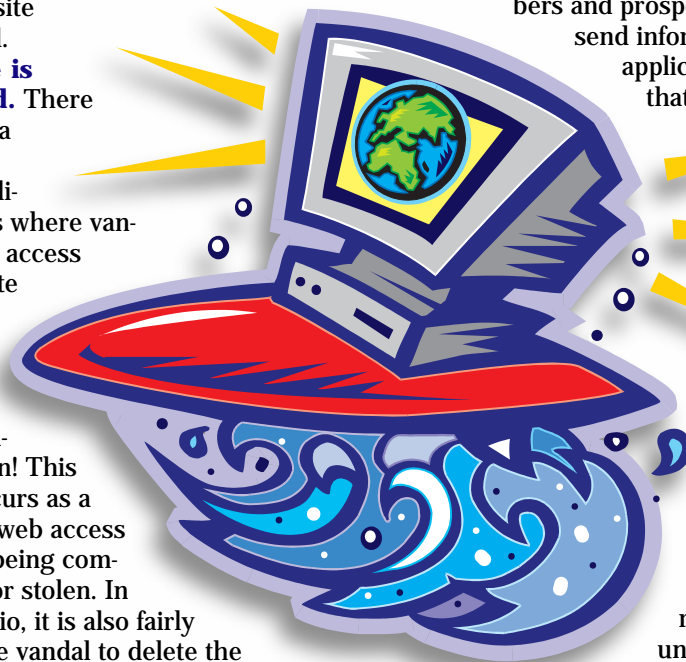
5. Identity theft. By its nature, Internet activity occurs in a relatively remote setting. Web sites are typically hosted at remote locations not part of the credit union. Our staff can go months without a physical meeting with a

web client. The institution can conduct many transactions without ever seeing the member or customer. There are two concerns here. We are concerned that CyFi employees are always dealing with an authorized employee or representative of the institution. Just as importantly, the institution itself must also concern itself with the veracity of information obtained from its web site. Is the person filling out the loan application really who they say they are? A relatively complex web site is likely to be made up of multiple components, and different third party firms may deliver those components. In that environment, it is particularly important to be aware of this threat.

6. Privacy and protection of customer information. Because the institution’s members and prospects do use the site to send information (say in a loan application), you must insure that this information is secure both when storing it on the web site, and when transmitting it over the Internet to the institution’s network or processing system.

7. Denial of Service (DOS) Attacks. This is an attack where a web site is bombarded with a high volume of illegitimate requests and is therefore unable to respond or responds slowly to legitimate requests. In this kind of attack, the data and integrity of a web site are never threatened, but confidence in its operation is thwarted when consumers cannot seem to reach the site.

8. Password compromise and “clear text”. The largest single exposure you probably face is the loss or compromise of passwords. An unauthorized person gaining access to a web-related password causes most of the bad things that can happen to a web site. Armed with a working password and an Internet connection, they can do quite a bit of damage and/or gain access to many things they should not see. For those reasons, we treat threats to passwords as a completely separate category. In particular, we are always



concerned when a password moves across the Internet in “clear text”. This refers to the fact that without encryption, email messages, web pages, requests to modify web pages, etc., all move around the Internet in essentially human-readable form. A competent hacker with lots of time and energy can wade through this traffic and discover passwords when they move in this unencrypted fashion. This, for example, is why we have a policy at CyFi of never sending a web access password to a client via email.

To protect your web site and its components, your web hosting firm or firms must do much of the work for you. But you have some responsibilities as well. We put the various remedies that are typically used into these two categories.

What Your Host Firms Can Do

1. Create backups for you; on-site and off-site. To protect against accidental site deletion, loss, physical disaster, or vandalism, regular and repeated backups of web site information must be made. At CyFi we do this twice per day; storing one copy on an internal high-speed server and making a second copy to tape and remove from the facility.

2. Monitor the network. A hosting firm has access to tools that can automate the process of scanning the network for potential security problems or breaches. In addition to insuring a network is running, these tools basically look for unusual activity levels and report those for manual follow-up. You should ask your host firms what they specifically monitor (for example - unsuccessful attempts to open up the web site for changes).

3. Use SSL for all remote data access. SSL refers to the ability for a web site and web browser to communicate using encrypted or scrambled data. Your host firm should be willing and able to use secure certificates and SSL technology for transferring any kind of data between end user and the web site. It is important to note that secure certificates can protect anything - logging on to remote banking, sending a loan application, or logging on for the purpose of changing the site. We strongly discourage any institution from taking application information over its web site without attaching and using a digital certificate.

4. Encrypt passwords to protect against compromised passwords. A host firm can encrypt all passwords when stored on servers accessible via the Internet or the firms internal

network. In the unlikely event that an intruder gains access to a file of passwords, it would require a significant amount of effort to decode them.

5. Communicate securely with clients. Make sure your host firm follows guidelines that make it difficult for an imposter to get information about your site. A favorite and very old hacker trick is to phone the network administrator, identify yourself by name as an employee of the credit union, and ask the network administrator to change a password for you.

6. Allow clients to update and modify authorized users. Your host firm is a potential password leak. While they may be involved in setting up initial passwords, make sure you always have the ability and responsibility to add and remove authorized users and their passwords. At CyFi, we are specifically not notified or aware that those activities are taking place unless, of course, a client requests assistance.

7. Protect the network with a firewall. A host firm’s network is normally going to be protected with a firewall of some sort. It is important to understand, however, that this is mainly for the purpose of protecting internal resources. Public web sites, by their nature, must exist and function primarily “outside” a firewall. A firewall does help protect against vandalism and potential password compromise by making it very difficult for an external computer to gain file level access to network resources. Note also that this refers to your host firm’s firewall and protection. It is perhaps more important that your own network be protected by a firewall.

8. Be able to reproduce your environment. For disaster planning purposes, your host firm should keep separate physical servers and Internet connections available. Should any of the existing public web servers completely fail, your site can then be re-deployed hopefully in a matter of minutes or hours.

What You Can Do to Protect Your Site

Protect your passwords. Unauthorized transactions or activities associated with a compromised password represent the biggest outside threat to your web. It is up to you and your employees to safeguard those passwords. The following traditional measures will help greatly:

1. Use a digital certificate to prevent clear text. Financial institution web sites

should have a digital certificate attached to it even if the site does not plan to offer on-line applications or other user-entered forms. A digital certificate allows the institution to perform all remote maintenance and data lookup using SSL or encrypted technology. Very simply, this dramatically reduces the possibility that an institution's passwords will ever be viewed across the Internet.

2. Insure password complexity. A complex password is difficult to guess. Our own network has experienced what is called a brute-force password attack. In these attacks, automated programs repeatedly try to gain entry using lists of commonly used passwords in the hope that they are able to find one that works. By making passwords a combination of letters and numbers, and by using passwords that are not likely to appear in a dictionary, this threat is reduced substantially. 'ccu3382' is a good password, 'cookies' is not. (A 7 character password, made up of 3 letters and 4 digits is sufficiently complex and also fairly easy to remember. Why? Find and read "*The Magical Number Seven, Plus or Minus Two*", George Miller's famous 1956 study on human information processing.)

3. Rotate passwords. People write passwords down, tell others for convenience, and otherwise make it pretty easy for co-workers and maintenance personnel to discover them. Because of this, regular password change and rotation is an essential security policy.

4. Delete unused passwords. With personnel changes, it is imperative to immediately change or update passwords that an ex-employee will already know.

Authenticate people who claim to be working for you. This one is deceptively simple. Have policies in place to insure your web operators and network personnel are sure they are dealing with the correct people when web activities are taking place. As mentioned earlier, a common method used to steal passwords is to pose as an authorized user.

1. Verify requests. If a network administrator gets a request for username and/or password changes or updates, the administrator should have a procedure to verify that individual if they don't know them personally or the request is not made in person. Callbacks and supervisor verification are two possible methods.

2. Verify third party individuals. Institutions regularly outsource web development and maintenance work. Make sure your internal administrators or webmasters maintain an authorized list of individuals named to perform web development activities. As with the previous item, separately verify requests for changes to usernames, passwords, or other security related requests that come from outside parties.

3. Monitor your content. While we at CyFi regularly monitor our network activity, we are not always in a position to monitor the quality or existence of content in a client's web site. You must make a habit and policy of constantly checking the web site and doing suggested quality assurance checks on the site. This regular activity will reduce the risk of inappropriate activity taking place without your knowledge. ♦



© 1999 Credit Union National Association, Inc. All rights reserved.

CUNA Technology Council Connected is a web-based newsletter published four times per year. Send news and CTC information to: Mike Pytlík, manager of technology, Communications Family CU, Saginaw, MI, e-mail: mikep@commfamily.org, phone: 517-249-8221, fax: 517-791-0281. For Council membership and administrative information, contact Cheryl Sorenson, manager - council administration, e-mail: csorenson@cuna.com, phone: 800-356-9655, ext. 4393, fax: 608-231-4061.



CUNA & Affiliates