CU t-t CREDIT UNION tech-talk
LEADER'S FORUM
SPECIAL ROUNDTABLE SECTION
TECHNOLOGY NEWS FOR CREDIT UNIONS SINCE 1988
WWW.CUNEWS.COM

# *Battling Security Fatigue – Working Towards Usable Security*

In today's world, more and more individuals are finding their personal information compromised in some way or another. In our credit unions we need to be sure that we do not exacerbate this situation by exposing personal information or providing a way that our systems could be compromised in order to do the same. One of the key factors in meeting this goal is security, but security can be a very tiring concept with which to keep up. Pure IT Credit Union Services has some insight on ways to help Credit Unions battle the fatigue of constant security awareness.

One of the most effective ways to combat security concerns, is to instill good security habits to the users and to make sure to educate those users as to the impact of security breaches and how they can affect the CU and the members. When instilling good security habits in credit union employees, the first thing that comes to mind for us would be Frequency. Habits are created through repetition and frequency. There must be frequent and regular testing - both announced and unannounced - as well as education. Credit unions are always pen testing but they need to be sure to institute social engineering testing as well. Regardless of the types and amounts of testing, education remains a top priority. CUs need to make sure that users not only see the habits they are trying to instill in them but that they understand WHY it is so important to practice safe computing. As service-based organizations, CUs want to help their members as much as possible, but they have to be sure that they are not allowing a security breach at the same time.

Oftentimes, users simply do not understand the value of the information that they are handling. They might think nothing of releasing particular information until you put them in the position to consider if it were their own personal information. It is really hard to put a dollar value on the information that they are handling and could potentially release, but that might help them to understand why we care so much. How much does it cost to pay out of a ransomware attack? How much would it cost if we found that some portion of our database were compromised and we have to inform the public about our breach? How much does it cost to have to replace every one of our credit/debit cards because of a database breach?

Another thing that we see is the need to model the behavior that we want to instill. We cannot have our helpdesk asking users for their passwords in order to help them. If we would never want that information revealed, then we should not ask for it either. Plus if we want to see longer or more complex passwords used, then when we suggest or provide a temporary password to someone we should provide a good example. While modeling the behaviors we expect from all employees may not be the perfect method to communicate to other employees the expected behavior, it does provide a solid foundation that can be used when explaining certain expectations.

It is also important that we understand that our security stance should be completely top down. We cannot make exceptions for the CEO or the members of the IT Department. All employees throughout the CU need to exhibit these same good security habits all the time. They need to become habits that we can model throughout the entire organization. If employees see that exceptions are made for certain people, then they will begin to feel that the policies shouldn't have to apply to them, either. This is the start to a chain that will eventually lead to the poor habits of an insecure environment.

*Continued on Page 2*

**Kyle Stutzman**
Vice President & Co-Founder

**Kyle Stutzman**
is Vice President Business Development & Co-Founder at Pure IT Credit Union Services Kyle has over his twelve plus years in the Credit Union space, and includes a stint as Chief Operations Officer of OGO, a Credit Union focused IT disaster recovery and community cloud provider. He holds an Executive MBA from Colorado Technical University and a Bachelor of Science degree from Eastern Mennonite University.

At Pure IT, we have built a practice around solving IT issues for Credit Unions. Our staff of experienced architects provide clear documentation and have open and transparent conversations to help Credit Unions understand what is working well, what may need improvement, what may be a business or security priority, as well as how much those improvements may cost. We are a Credit Union Services Organization or CUSO, this helps us stay focused on solving IT problems that are unique to Credit Unions.

***Contact Info***

***www.pureitcuso.com***

CU t-t CREDIT UNION tech-talk
LEADER'S FORUM
SPECIAL ROUNDTABLE SECTION
TECHNOLOGY NEWS FOR CREDIT UNIONS SINCE 1988
WWW.CUNEWS.COM

# *Battling Security Fatigue – Working Towards Usable Security*

But we also have to battle the security fatigue in our end users, not just in the IT department. One way we have found is to change from passwords to passphrases. In our opinion, all of this constant password changing and complexity simply makes for less secure passwords because the users will just add a number to the end that they change each time or they will start writing them down on a note under their keyboard. If we use a longer passphrase then it becomes both easier to remember and more secure. Mathematically, forcing an uppercase letter and a number into a password is less secure than having an additional 2 characters added to the password. If we can push for a phrase that is 16-24 characters long then it becomes much more mathematically complex to crack the password. That reduces the constant changing and forgetting of passwords which reduces the security fatigue our users and IT departments see.

Another option is to move to certificate-based authentication which allows for systems to identify each other and reduce the number of times for which a password is requested. Individual users can use a password manager tool that can centrally retain complex passwords for each system to which the user needs access. The tool can then be unlocked by a single complex passphrase, giving them access to all of their stored passwords/passphrases. With this type of tool, users can maintain adequately complex passphrases for many different systems without needing to keep memorize all of those separate passwords.

Finally, from a human perspective, we should develop a culture that does not make our end users feel stupid for asking a question. We should reward our users for each time they call into IT and ask about a suspicious email that has arrived in their inbox. We want to know about these things so that we can better protect against them. We could even go further and encourage people to report on security issues and concerns, and then reward them with prizes.

As a Consulting and Managed Services organization, literally everything we do is delivered with security in mind. Security is a core component of every engagement we are involved in. But we still have to get users to take the right actions. We do that by providing policy based infrastructures. One of our common solutions is what we call our Pure Micro Cloud. Basically we are building a self-contained private cloud solution that contains all of the features of the big public cloud solutions, but with dedicated hardware and software for a single organization. A core building block of that is policy-based infrastructure where when someone provisions a new server it comes with the necessary security policies turned on; a policy-defined virtual network deployed with the proper security design; and a virtual firewall with security policies already enforced. Designing an infrastructure within a virtual environment gives us this level of abstraction that allows a better view across much more of the infrastructure and hosts, as opposed to attempting this with disparate individual tools.

We also build our solutions complete with Single Sign On within the environment, including having a secure Wi-Fi network authenticated with your same login password. Just contemplate that if you have a public and private Wi-Fi environment but someone gives away the private Wi- Fi access. Normally if you want to resolve that issue, you would need to force every user to change the access code in every single device. If an employee leaves the CU, you would need to do the same thing. Everything needs to be authenticated through the user's individual authentication, and these tasks are much easier to accomplish within a virtual environment.

We also specialize in building and deploying Virtual Desktop Infrastructures throughout organizations. This gives us the same sort of granular oversight and control over employees' desktops. We can ensure that every desktop is the same golden image. If a user does manage to do something to their profile, we can just roll it back to the good image. We can easily build new desktops that comply with your Group Policy requirements, and suppress updates that might affect critical apps that need to stay at a certain revision.

In regards to network virtualization, we utilize network virtualization technologies, such as VMware NSX, which allows the entire network to be virtualized and abstracted. The hardware underneath is simply providing packet forwarding and physical connectivity at this point. This means that every network is deployed with the correct security, VLANs, and connectivity.

**Kyle Stutzman**
Vice President & Co-Founder

**Kyle Stutzman**
is Vice President Business Development & Co-Founder at Pure IT Credit Union Services Kyle has over his twelve plus years in the Credit Union space, and includes a stint as Chief Operations Officer of OGO, a Credit Union focused IT disaster recovery and community cloud provider. He holds an Executive MBA from Colorado Technical University and a Bachelor of Science degree from Eastern Mennonite University.

At Pure IT, we have built a practice around solving IT issues for Credit Unions. Our staff of experienced architects provide clear documentation and have open and transparent conversations to help Credit Unions understand what is working well, what may need improvement, what may be a business or security priority, as well as how much those improvements may cost. We are a Credit Union Services Organization or CUSO, this helps us stay focused on solving IT problems that are unique to Credit Unions.

***Contact Info***

***www.pureitcuso.com***