

## WHY YOUR USE OF ID AND PASSWORD IS LIKELY A JOKE

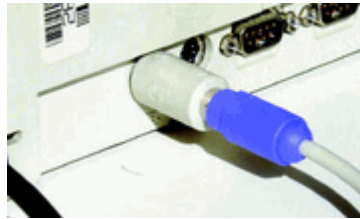
### WHY YOUR USE OF ID AND PASSWORD IS LIKELY A JOKE

When you went to work this morning did you use a id and password via the keyboard to log on to your enterprise's systems? When you use your bank site, are you entering in a id and password via a keyboard? This paper will conclusively show you why your use of ID and password is likely a joke.

**How easy is it to obtain another person's id and password? IT'S VERY EASY AND THERE ARE MULTIPLE WAYS OF DOING IT.**

#### ATTACKER OPTION #1: NO FUSS, JUST 10 SECONDS TO INSTALL

What does this look like?



It looks like a piece of computer hardware...right? Wrong! It's a hardware keyboard logger. It stores everything you type into the computer including you id and password. It's a device that simply plugs into the end of your keyboard and into the computer. [They're legally sold for \\$60 or more.](#) It takes about 10 seconds to install. In fact, a child can do this.

During the past year in the US, several students have been caught in different schools including [Houston](#), [Palm Beach](#) and [Boston](#) using the keyboard logger to download their teacher's id and passwords. One had spent two years changing marks for friends so they could get into university.

In the [UK in 2005](#), a group of criminals paid janitors to install them on different computers in a bank. They obtained id's and passwords for key employees. They were caught when they were transferring portions of \$220 million pounds to a bank account.

This type of device is almost impossible to detect for the normal user. Further, the normal enterprise monitoring systems won't detect the device either since it doesn't install any software on the computer. The criminal simply unplugs it, takes it back to their home, plugs it into their own computer and downloads everything you typed over the past days, weeks or even months! They now have your id and password.

## WHY YOUR USE OF ID AND PASSWORD IS LIKELY A JOKE

### ATTACK OPTION #2: SOFTWARE MALWARE KEYBOARD LOGGER ATTACK

You receive an email from a friend, or a site advertising its wares. In the email is a link to click on. When you click on the link you are taken to the site and everything to you looks normal...BUT IT ISN'T!

The email link you clicked on automatically downloads some software to your computer. This software is nowadays very sophisticated. It can quickly penetrate most computer defences and install itself on the core operating system of your computer. Once there, it quietly sets up shop and waits for you to enter in ids, passwords and credit cards. As you enter in this information, the software then immediately sends it to a criminal gang. This is known as malware (short for malicious software). What are the chances of this happening to you? **THE CHANCES ARE VERY HIGH!**

For example, in [March 2006](#), Russian organized crime used rootkit software. This places malicious code at the heart of the Microsoft operating system. The code was installed when a user visited certain sex websites. It then watched for when a user entered uid and password information for banks, dating, social websites and email. As the data was entered, in seconds, the rootkit software then began passing the information back to a Russian web server. Over four day's time **90,000 pieces of user information from 6,500 companies was sent before the server was shut down.**

Organized crime now sells millions of uids, passwords, social security and credit card numbers in eBay type auctions. For example a web mob named Shadowcrew: [“In the past two years, the Shadowcrew's 4,000 members, according to the U.S. Secret Service, ran a worldwide marketplace in which 1.5 million credit card numbers, 18 million e-mail accounts, and scores of identification documents—everything from passports to driver's licenses to student IDs—were offered to the highest bidder.”](#)

As well, the code for writing these types of attacks has become modularized. This allows the criminal to effectively order a piece of code that performs specialized functions. Further, the code can be checked before purchase by the criminal to ensure it will bypass the enterprise's existing intrusion detection systems. [Code is being offered at \\$25 per 10,000 hijacked computers it infects.](#)

[McAfee in April 2006](#) stated that the increase in Windows based stealth components was 2,300% from 2001 to 2005. Authorities estimate that today in the US there is on the order of 20-40 million infected computers.

Starting to feel a little queasy about using id and passwords as a security mechanism?

## **WHY YOUR USE OF ID AND PASSWORD IS LIKELY A JOKE**

### **ATTACK OPTION #3: DICTIONARY ATTACK**

How much computing power is required to hack a password? The most common way is to do a dictionary attack. This method has the computer try out every kind of word and variation thereof against a password. [This site](#) will show you that a normal every day computer can do about 10 million passwords per second. A workstation can do 100 million per second.

The time it takes can range from a few seconds to a few days on most commonly used passwords of 8 to 10 characters. In other words, your password can generally be easily broken if the attacker has access to your password entry and isn't stopped after three attempts. This same attack also applies to documents, spreadsheets and database passwords.

### **ATTACK OPTION #4: SOCIAL ENGINEERING ATTACK**

Why should a criminal work harder than they have to? One of the easiest ways to obtain your password is to get it through social engineering. Many people have lists of passwords attached to their terminal, under their keyboard or in a side drawer or book.

If this method fails, the criminal can use what's called an over the shoulder attack. In this method, the criminal either watches or points a piece of their clothing that contains a miniature camera at the keyboard and watches what you type in.

### **ATTACK OPTION #5: JAMES BOND METHOD**

Then there's the option to a criminal to use some high tech toys to obtain your id and password without being in the room. This approach uses the sound your fingers make on the keyboard to obtain the actual keystrokes. The intelligence agencies have been using this tactic for many years. It's one of the reasons why high security buildings don't usually have glass windows.

Well, the age of spies is now coming to you. Last year scientists from the University of California showed a [study](#) where they can obtain 96% accuracy for words typed in English on a keyboard. What this means is that the technology to do this is now within reach of criminals. They point a sound dish at an office window, record the sounds of you typing, process it on their computer and voila! They now have you id and password.

### **THE USE OF PASSWORDS AS THE PRIMARY SECURITY MECHANISM, ESPECIALLY WHEN ENTERED IN VIA A KEYBOARD, IS DEAD!**

The enterprise risk is very high when using passwords. Additionally, the risk to the end user is equally high, especially when their personal identity data is at risk. What is the solution?

## **WHY YOUR USE OF ID AND PASSWORD IS LIKELY A JOKE**

### **YOU'RE IN A ARMS RACE**

There is no silver bullet that will solve the enterprise risk from passwords. The reality is your enterprise is in an arms race where right now, the advantage is clearly with the opposition. Criminals now have sophisticated development tools, personnel and large pools of computers they control (botnets) to bring attacks to your doorstep and beyond the firewall.

You therefore need a layered strategy to deal with this. Given the current state of the arms race, you must assume that your outer enterprise defence layers will be breached despite the best efforts of your systems, staff and vendors supplying firewalls. You must therefore use greater security for each part of the enterprise where the risk is high.

### **A LAYERED IDENTITY ENTERPRISE SECURITY STRATEGY**

I recommend a nine level identity enterprise security strategy:

#### **FIRST LEVEL OF DEFENCE: IDENTITY REGISTRATION**

When an employee comes to work for you, what kind of identity check did you do on them? Was there any criminal record check? Did you check out their education credentials? Do you do any kind of criminal or education background check on contractors and consultants working for you? What kind of identity check do you apply to customers who will be using your systems?

As the enterprise risk rises for applications and information systems your customers will be using, so to must the initial identity registration check increase. This level of first line defence is usually poorly thought out in most enterprises, especially beyond employees.

#### **SECOND LEVEL OF DEFENCE: USER TRAINING**

Does your enterprise do any kind of annual training for all users of your systems about email, phishing and rootkit attacks? Are you strongly warning them about the danger of clicking on any links in an email document? This kind of basic training, while it might be ignored, put's some of the enterprise defence on the shoulders of its users. A 2-3 minute online flash presentation can be put together cheaply. It may result in your enterprise being able to avoid an enterprise breach.

## WHY YOUR USE OF ID AND PASSWORD IS LIKELY A JOKE

### THIRD LEVEL OF DEFENCE: DEVICE SECURITY CHECK

When a user tries to log on to your enterprise systems, is there a device check done? Is the software and hardware platform checked out and ensured that all available patches are in place? If not, before the device can even reach your network, is it placed in a quarantine area where patches can be recommended to be installed? If you're not doing this, using a device like from [Caymas](#), then your enterprise is open to unexpected forms of attack.

### FOURTH LEVEL OF DEFENCE: INITIAL IDENTITY AUTHENTICATION

Your users, if you're going to require password authentication (which is the weakest form of authentication) should enter in their id and password using a keyboard less entry. Companies like [RSA](#) and [Bharosa](#) provide excellent tools allowing you to minimize the risk of keyboard hardware and software attacks. **DO NOT USE KEYBOARDS FOR PASSWORD ENTRY...IT IS TOO RISKY TO BE CAPTURED.**

The initial authentication, if only using id and passwords, must only allow the identity basic, low risk access to specific pieces of the network, applications and information. **Do not trust the authentication for medium and high risk enterprise applications.**

Further, if the user is coming in via a wireless device are they given more restricted access privileges than if they are logging on from inside the enterprise? If not, then you should be rethinking your enterprise security strategy. Wireless devices authentication methods are relatively easily breached. Therefore, limit your enterprise risk by either restricting access to low risk applications or, requiring stronger authentication from the user in order to access higher risk networks, applications and information.

### FIFTH LEVEL OF DEFENCE: QUICK PROVISIONING AND DE-PROVISIONING

When a user no longer requires access to your enterprise, an application, building, room, network, etc., how long does it take until they are de-provisioned? Many enterprises have very weak to poor provisioning and de-provisioning processes. In today's age, this puts the enterprise at greater risk, since a user who is gone may still have access to the enterprise. Put in place the infrastructure to quickly add, adjust or remove someone from having physical or electronic access to your enterprise

## **WHY YOUR USE OF ID AND PASSWORD IS LIKELY A JOKE**

### **SIXTH LEVEL OF DEFENCE: STRONGER AUTHENTICATION**

As the enterprise risk rises for networks, applications and information access, so too must the level of authentication strength. The financial system, payroll and payables are all higher risk. So too are users who hold super-user privileges like senior network administrators.

For all of the medium and higher risk applications, your enterprise should be using a graded series of stronger authentication. For instance, low to medium risk might be addressed by the user providing their id, password and a digital certificate. Medium risk should be addressed by the user providing things like a secureID token along with their id and a password. Medium to high risk should be addressed by the user providing something like a smart card, a secure id token, a biometric and a second unique password.

Can your existing security and identity sign on systems support this? Do you have budgets for this? All of this requires senior management support to successfully implement.

### **SEVENTH LEVEL OF DEFENCE: RE-IMAGING NETWORK OPERATING SYSTEMS**

Are you prepared for a successful rootkit attack against your enterprise? Currently, Microsoft is recommending that the best way to recover is to re-image all desktops and servers affected! This could bring your IT department to a halt. Are you prepared for this?

Don't rely upon the firewall and the vendors. While they will assure you of their defensive abilities, the chance of an attack getting underneath the firewall is currently a lot higher than they would let you believe. If you are the unlucky enterprise who gets hit by a rootkit attack before the firewall vendors figure it out, then you had better be prepared to deal with it and fully recover, quickly and at low a cost as is possible.

## **WHY YOUR USE OF ID AND PASSWORD IS LIKELY A JOKE**

### **EIGHTH LEVEL OF DEFENCE: TRANSACTION AUTHENTICATION**

The emergence of numerous attack vectors on an enterprise means that enterprise must assume that criminals will successfully penetrate their outer layers of defence i.e. the firewall and the authentication systems. The answer to this is to deploy transaction authentication.

In transaction authentication, software watches the following:

- IP address being used by the user
- Geo-location of the user
- Time of day the event is occurring
- Historical user pattern
- Computer hardware the user is using

If any of these criteria are different than expected, even with a successful authentication, the transaction authentication software will start alarm bells ringing in the enterprise.

This may result in:

- The user being asked all sorts of personal questions to verify it is really them
- Security or business managers being paged in real time
- The event, process or transaction refused

All enterprises should be using this type of software to protect high risk applications like payables and other sensitive applications. [RSA](#) and [Bharosa](#) are recommended vendors.

### **NINTH LEVEL OF DEFENCE: ENTERPRISE REAL TIME AUDITS**

The final layer of defence is the ability to quickly go back in minutes, hours, days, weeks or months to find out every network, application, information resource, type of device used, building and room the identity used at a specific point in time. All too often, the audit data is very hard to interpret from a application audit trail and worse, hard to integrate with other audit data from other applications.

Get a team organized on trying to provide an end to end user audit that is quickly available, easy to access and use. This will help you find out where problems and breaches occurred and then prepare remedial action.

## WHY YOUR USE OF ID AND PASSWORD IS LIKELY A JOKE

### RECOMMENDATIONS FOR USERS

All of the above doesn't help if the enterprise chooses to ignore the recommendations. Therefore here are my recommendations for you:

1. Start demanding of any institution or company you deal with to change their methods of authenticating you. Get public campaigns together and tell the banks, merchants, governments and others that your identity information requires them to adjust to the times. Demand they provide you with either keyboard less entry and even better, multifactor authentication.
2. Begin to sue companies who ignore your requests. It's only when the companies feel the dollar hit from lawsuits from its users re authentication methods and their identity data that they will change. Today, if you're a small time user, the company will simply accept the risk that your account might be broken into. While this might make good sense from the company's perspective, it does you no good when your identity data is compromised.
3. Don't click on any email links. This is one of the main routes to launching malware attacks. The current risk is very high that your computer may become infected with malware.
4. Write emails and letters to the politicians demanding that they tighten up laws pertaining to user authentication. Demand that they begin requiring companies to use multi-factor authentication.

### CONCLUSION

The last several years has seen a change in attacks. Mostly gone are the days of "hackers" just trying to prove a point that they are smarter than you and can crack your defence. Today, we're in the age of cyber criminals.

The cyber criminals operate globally and locally. They are constantly on the prowl for enterprises that are easy take-downs. Whether it's employing janitors to install the keyboard logger on targeted computers or students wanting to download their exams in advance, it really doesn't take that much effort to crack existing enterprise defences.

While the financial industry is slowly responding by implementing transaction authentication and multi-factor authentication, most other industries are still operating a defence strategy that would have worked well ten years ago but not today. It's time to wake up and smell the electrons. Smell the attacks coming and get ready to handle them before they handle you. Implement a layered enterprise identity strategy.

## **WHY YOUR USE OF ID AND PASSWORD IS LIKELY A JOKE**

### **ABOUT THE AUTHOR:**

Guy Huntington, President of Huntington Ventures Ltd, has many years of experience leading large, complex, Fortune 500 identity projects. His work has included leading Boeing's single sign on, Capital One's single sign on, Capital One's Sarbanes-Oxley provisioning project and Kaiser Permanente's web single sign on review.

He maintains a website on authentication at [www.authenticationworld.com](http://www.authenticationworld.com) . He also maintains an authentication blog available off his website. He can be reached at [guy.huntington@authenticationworld.com](mailto:guy.huntington@authenticationworld.com) or by phone at 604-921-6797.