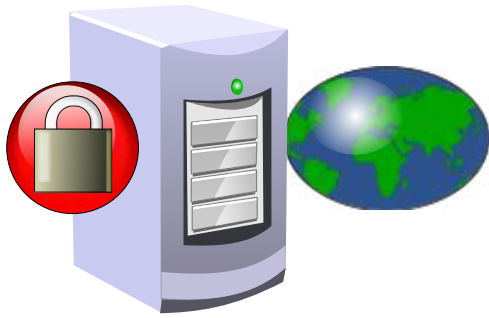


Basic Internet Security Precautions

By Greg Bahlmann



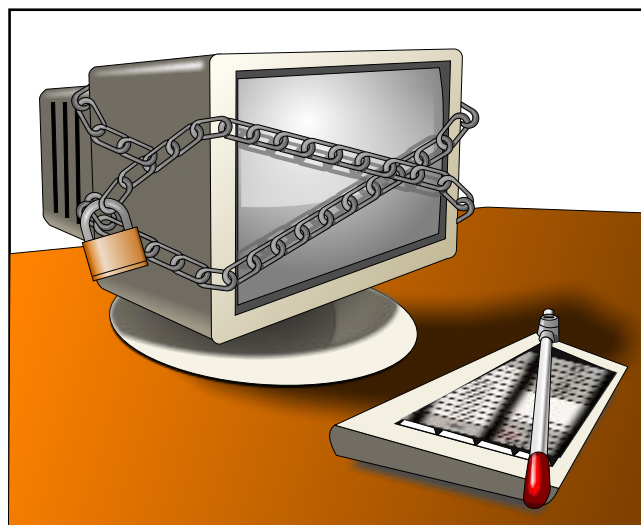
Brought to you by:



www.ezbizsa.com

In light of the numerous scams being perpetrated on an unwary Internet community, especially in South Africa, I have written this article help inform the many people who spend time online and are unaware of the potential risks of using the Internet and e-mail. I do not want to be a “prophet of doom” and scare you away from the Internet but like many things, you need to know the risks and how to avoid them if you are going to get the most out of your time online. In short, I hope that what you read below will make you a more confident web surfer.

How do you think most web-related crimes are committed? We often see a pimply faced teenager hacking into the Pentagon’s computer in the movies and so you would be forgiven for thinking that most cyber-fraud or cyber-theft is committed by hackers (or “crackers” as they are referred to by people in the know). In real life, however, the facts are a little different. According to the IC3 report on Internet fraud for 2008, 74% of online criminals are using e-mail as their contact method while only 29.9% used web pages (“hacking” websites through a variety of methods). The report also states that South Africa ranks 6th in the list of online fraud perpetrators, although the percentage of the total number of perpetrators is estimated at only 0.7% of the total, with a massive 66% being from the USA. However, when one looks at the fact that over US\$ 264 million was stolen through the Internet in 2008, even a small percentage of the “crime pie” still makes a sizeable sum - especially if it’s your money that has been taken. You should also bear in mind that the complaints used to draw up these statistics were almost entirely sourced from the USA and so it is not a true reflection of the online crime situation, especially in South Africa where statistics for online crime are almost non-existent. However, it is an indicator and a scary one at that!



Much is made of Internet security for companies as far as securing their online resources against viruses and hackers but little regard is paid to the Internet user who is not familiar with the tricks and scams being perpetrated on the Web or the procedures to follow to stay safe online. In fact few companies post security information for the users of their websites and if they do, most simply offer security guidelines that are often too vague and/or technical for the average person to make sense of. Often these guidelines are buried in amongst the articles on the site and will only be found by visitors to the website that are determined to find the relevant page. In our view, this is not good enough. It should be the responsibility of all companies that do business on the Internet to educate and inform their customers and visitors to their website(s) about what risks are out there and what they can do to counter them.

Nowadays, online scams (through which people are duped to reveal their personal details - which are then used to access their bank accounts - or persuaded to make payments that they should not be making) are less likely to be purely Internet based, although the Internet is where the attack usually begins and that is where the damage is often done. Cyber criminals are employing everything from cell phones to faxes, letters to personal contact to commit their crimes. As companies employ more and more security to foil the online criminals, so many of these scams are becoming more and more intricate, even to the point of being ingenious.

And it is the person in the street who is at risk of being defrauded. It is with him or her that we find the greatest need for online security while online. And it is through simple awareness and circumspection that the Internet user can avoid the many scams roaming the Web. Never before has knowledge been so keen an adversary of crime.

Below is a list of precautions that I have drawn up to safeguard the average Internet user. Obviously I cannot (and do not in any way) guarantee that you will never fall victim to cyber crime but following these precautions can at least give you a fighting chance and help keep you safe for most online activity.

Precaution 1: Don't Use Public Internet Access to Log into Internet Banking!

No website is infallible, no matter how good the company running it says their security is. Yes, even banks are prime targets for Internet criminals. In a place like an Internet café, a library or airport where anyone has access to the computer it is a huge no-no to log into any site that contains your personal information, especially one containing sensitive data like bank account numbers. Internet café computers are notoriously corrupt and criminals will often load software onto these public machines to store usernames and passwords, which are later retrieved and used to access whatever sites the unsuspecting victims logged into from the machine used. We would go so far as to say don't even log into webmail (like Gmail or Yahoo!mail) or social sites like Facebook from these public machines.

Precaution 2: Be Careful When You Go Wireless

As an addendum to the previous point, don't use public wireless connections in coffee shops or other places for secure transactions as these can be accessed with the right equipment. It's fine to use these connections to surf the web but think twice before paying for anything online.

Precaution 3: Check the Lock



An example of things to check before registering with or logging into a website; the “https” in the website address and the secure padlock.

When logging into any secure environment like a banking website, make sure that the log in page’s web address starts with “https” (“https://www...”) and not just “http” (see the image above). That “s” denotes that the communication between your computer and the server is secure. There should be a small lock icon at the bottom of the web browser and some web browsers have a coloured bar to the left of the web address that also shows that the page is secure. If you click on the lock icon, you will be able to view the SSL certificate that confirms that the site is secure. This does not guarantee that the website itself is completely safe but it is at least a good start.

Precaution 4: Check the Web Address

If you are logging into a website to conduct a transaction, apart from the things to look out for in Precaution 3, take a quick look at the site’s web address in your browser’s address bar to make sure that it at least looks legitimate. A company website should have a clear domain name like <http://www.companyA.co.za>, after which may come various other words and symbols (such as <http://www.companyA.co.za/public/index.asp>). Most companies will have a domain name that is the same as their company’s name, although some don’t because these names have been registered by opportunistic people before the company could register it or other companies with a similar name has bought it. However, the web address will usually be something similar to the company name or something related to something they do or sell. If you aren’t sure, it’s worth a call to the company to find out. However, try to find the telephone number in a source other than their website (like the Yellow Pages or even another website) because the number may be phony if it’s on a fake website.

For example, let’s say you want to deal with company A. The web address you are using should be something like <http://www.companyA.co.za> and there may be a few things after that, as mentioned above. The important part is what comes before the .co.za, .com, .net, .org (called the top level domain) or whatever else it might be. It should be the company name or something similar.

Some companies may be using a hosted solution like EZBIZsa and so may have a website address like <http://companyA.ezbizsa.com>. This is called a subdomain address. In such a case you should be able to go to the hosting company's website (like EZBIZsa) to see if they exist and then to confirm that the site of the business you want to deal with is in fact a part of their system.

However, if you are looking onto a company's website and see a long string of "gobbledegook" like <http://companyA.hellosites.com/d/fwd.asp?x=companyA&other=divert> ... you should have your guard up. Looking at the address, we see that the important part is the name before the .com in the address – in this case "hellosites". If you type in <http://www.hellosites.com> you will be taken to their website. If it is blank or is just a directory-type of site then beware. Another type of address to stay away from is the one with numbers (IP address) instead of words after the <http://> in the address. So if you see the address is <http://203.154.764.128/def/index.asp> watch out! No legitimate company would use this type of web address unless they were hiding something.

Precaution 5: Use Firefox

Think about switching to the Mozilla Firefox web browser if you are still using Internet Explorer. Firefox is free and far more secure than Internet Explorer (although the Internet Explorer pundits might disagree). And if you couldn't be bothered to change, at least upgrade your browser to the latest version. So if you are still using Internet Explorer 5 or 6 you are looking for trouble as they are notoriously "cheesy" (full of holes).



If you would like to download Firefox, go to <http://www.mozilla.com/en-US/firefox/upgrade.html> to download it.

Precaution 6: Don't Follow Links in Suspicious E-mails

This is how a lot of people get caught out. They get an e-mail from "their bank" asking them to click on a link to "their bank's" website. Once there, they are asked to verify their personal details or do something similarly revealing. The e-mail may look legitimate, as does the link they are asked to click and the site they are taken to may even look exactly like the bank's real site. However, what appears to be the bank's website is actually a mock-up and when the unsuspecting victim logs in, their username and password are stored and used by the criminals who set the scam up to enter the victim's real online bank account and steal the money they have there.

Banks and other companies *should* never ever ask you to verify details or log into their website. They will never *ask* you to do anything important by e-mail. If you get a message like this and you are not sure if it is legitimate or not, phone your bank and ask about it before doing anything. Again, if you don't know the number look it up in the phone book or at least search for your bank's website in a search engine like Google or Yahoo! Don't use the numbers listed on the site that you went to from the link in the suspicious e-mail.

Another precaution that can be taken here is to look at the bank website's web address and apply the

considerations listed in Precaution 4 above. These types of scams are called “phishing” scams and come in many forms.

Precaution 7: Check the E-mail Address

If you get an e-mail from your bank asking you to log in to their website and change your contact details, quickly check the e-mail address that the mail came from. If it is from a Hotmail or Yahoo! e-mail address or even one that doesn't have anything in common with the bank that supposedly sent the mail, then delete the mail – or if you have a guilty conscience, phone them to check.

Precaution 8: This May Seem Obvious ...

The truth is that if you receive an e-mail in which some official of a remote country asks to store money (usually a large sum) in your bank account for a weekend in return for a million dollars, it's a scam. These sorts of things just don't happen. If you hand your bank account details over, you are going to lose your money. Any deal that seems too good to be true IS too good to be true. However, naïve people still get caught with these scams, even in this day and age.

Precaution 9: Beware of the Unsolicited Attachment

If you get an e-mail from someone you don't recognize with an attachment (an attachment is a file that accompanies an e-mail. You must click to download the attachment to your computer where you can open it) delete it out of hand – especially if it promises free porn or a deal that's too good to be true. Most e-mail systems can now clean malicious e-mails but their attachments could very well contain a virus that will infect your computer when downloaded and opened. This is how many computer viruses are spread nowadays. Sure, it may be legitimate but it's not worth the risk.

Precaution 10: Don't Store Important Passwords in Your Phone and Don't Keep Them in Your Wallet/Purse Either

If your phone or wallet/purse get stolen, the thief can peek at your important info and log into your accounts if he has some initiative. So where do you keep passwords? If you are like me, you have loads of passwords and it would be impossible to remember them all. I have had them tattooed backwards onto the soles of my feet so I can read them in a mirror. No chance that any criminal is going to get close to my sweaty feet on a hot day. It's a personal choice but it helps to be devious. Many people I know write all their passwords in a small book that they hide away on their desk. That way they have all their codes in one place and it isn't on their computer (which could get broken into, stolen – or hacked). Obviously the book could get stolen when nice Mr. Thief visits you in the dead of night and so it is important to put it somewhere not too obvious.

Precaution 11: Don't Use the Same Password Everywhere

Many people use the same password (usually their birthday) for all of their online accounts because it is easy to remember. Uh-oh. When nice Mr. Thief finds out one password he tries his luck at some other places he thinks you might be a member - and voila! He has access to your virtual life. Then suddenly your bank account is empty and your Facebook gallery is full of pornography.

Precaution 12: A Secure Password

There are dictionary programs out there that can crack a password made up of only English words or names in a matter of minutes, so it's important to use difficult to guess passwords that would not appear in the dictionary. What is more, your passwords should be at least eight to sixteen characters long (the longer, the better) and contain more than one capital letter and a few numbers. You could just use random numbers and letters – like F5bs91Xw95lq - but the problem with that is that it's difficult to remember unless you have a head for that sort of thing. I usually use a word or words that I will remember and alter it/them to make it harder to guess – like baZoo5kaf9iSh (“bazooka” and “fish” with a few numbers and capital letters thrown in).

Precaution 13: Get an Anti-Virus Program for Your Computer

Viruses are becoming a bigger and bigger threat as the Internet becomes more and more important. They live inside millions of computers without their owners ever realizing it, siphoning off information and sending it to the virus' creator or acting as a transit point for computer code to attack government and corporate networks. It is therefore essential that every person take responsibility for their own computer's security. Decent anti-virus software is available for free (such as Komodo firewall) although paid-for software is always better. We use NOD 32 which is extremely good, easy to use and inexpensive. Make sure that the software you choose has a firewall, an anti-virus capability that is updated regularly (at least once a day) and an e-mail scanning capability. And don't use pirated security software as you are playing with fire. Rather get the free software.

Precaution 14: If You Are in Business, Draw Up a “Communication Security Declaration” (CSD)

Companies big and small can help minimize the risks for their customers by creating a set of guidelines for communications with them, both online and through normal channels and then distribute it to their customer base in printed format. In it they can advise customers how to contact them, exactly how they will be contacted by the company, the people who will be communicating with them and the communication formats to be used. The company should then stick to these guidelines rigorously to reduce the chances that criminals will find ways to perpetrate scams.

The effect of the Communication Security Declaration is that the chances of success for a criminal masquerading as an official from a particular company that is the target of their fraud would be reduced. A cursory check against the CSD would reveal that they are not authorised to request information or request that information be altered.

The CSD is a fairly new idea and would differ from company to company, depending on how risky their communication processes are perceived to be.

Precaution 15: Be Careful What You Post on Facebook and Twitter

Cyber-criminals (and normal criminals for that matter) are starting to trawl through social sites like Facebook to glean whatever information they can from what is posted there about people.

Imagine this scenario. An avid techno-junkie, Bob Smith, posts information about where he works on Facebook and his gallery is full of pictures of Bob, his family and his home. A criminal finds Bob by simply going to where he works and, knowing what he looks like from his Facebook gallery, follows him home. He now has his home address. Along comes the holiday season and Bob and the family are off

overseas. The criminal now knows this because he followed the link from Bob's Facebook page to Twitter and sees Bob's tweets about how he is looking forward to the trip, where they are going and for how long they will be away. Bob continues to tweet when they depart, describing their flight, their hotel in a far away country and so on. The criminal now knows he has all the time in the world to burgle Bob's home.

The criminal with initiative can use the information they find on the social websites to craft ingenious scams and so it is essential that you limit what you post there.

This type of precaution can also help foil "cyberstalkers" who prey on vulnerable people through the social websites. There have been cases of cyberstalkers getting people (usually the young and impressionable) to do terrible things like pose nude for them online or even kill themselves. Cyberstalkers also pretend to be someone else and convince their victim to meet up with them, after which they sexually assault them. This type of crime is especially worrisome for parents and if you have children who go online, try to monitor what they do and where they go on the Internet. There is software available that can restrict access to certain websites and so protect younger web surfers.

Precaution 16: Never Give Out Your Personal Details

The only time you should EVER type your personal details (name, address, credit card number etc.) into a website is if you are 100% certain that it is a legitimate site and is properly secured (following the guidelines above). If you are not sure, don't enter them into the site. And never, never send your details to anyone via e-mail. E-mails are not secure.

Precaution 17: That Tearful E-mail Appeal by the Mother of the Dying Baby is Most Probably a Scam

Every year, thousands of people fall victim to scams involving heart-wrenching appeals for donations to save unfortunate people in remote parts of the world. It is unfortunate that we cannot trust these appeals any longer as there are most probably many people who have legitimate needs and who have been sidelined by the fraudsters. However, don't reply to these e-mailed appeals and don't send them on.

Precaution 18: Log Out

Almost everyone using the Internet will log into a website's password-protected area at one time or another. Many people doing so will simply close the window they are working in when they are finished and will not log out. This can be dangerous as sessions used to validate the user are left intact, at least for a short time and can be used by people who know what they are doing to view your details or transact on the site you just left in your stead. The chance is small, but it exists. So, do yourself a favour and log out! Sometimes the log out button is small and hard to find, but take the time to look for it and use it.

Scam Examples:

Below are some examples of scams that have been perpetrated in the real world, just to give you a taste of how the criminals really function.

1. The Website Logo/Fax/Bank Insider Scam

Company A built a website on which they displayed their logo – as many companies do. The criminals in question took the logo from the site and created a legitimate-looking fax using the header. They then phoned Company A and managed to get information about the company which they used to open a bank account in Company A's name (presumably with the help of an accomplice in the bank). They faxed Company A's clients and told them that in future, money owed to Company A should be paid into the new (scam) account, which some of the client companies did.

Suggested Precautions

In this case, a Communication Security Declaration with provisions that clients would not be advised of the change of company or banking details by fax or e-mail and asking them to verify any changes of such a nature by phone, would have reduced the chance of such a fraud.

2. The Internet Banking/Cell Phone SIM Card Swap Scam

Mr. A was away on holiday over Christmas and popped into an Internet Café to do some online banking. Unbeknown to him, a program planted on the computer he used stored his login information. The criminals were able to access his bank account online but couldn't steal any money yet as they knew a confirmation SMS would be sent to his cell phone. However, using the details they got from his online profile on the bank's website, they were able to find out what his cell phone number was and then arranged to do a SIM card swap (which South African cell phone companies permit with relatively little red tape involved, sad to say) so that they now had his cell phone number. They then logged onto his online banking account and transferred all the money out of his account as well as his small business account which was linked to it. An SMS was sent to "his" cell phone but it went to the thieves instead, who were able to retrieve the confirmation code from the SMS and entered it, concluding the transaction and stealing the money.

Suggested Precautions

Never log into any password-protected site or do any transacting by buying anything online on public computers or on free wireless connections in public areas or shops.

Conclusion

We hope that this article has been interesting to you and that you learned something new. Security is an important part of being a "netizen" (online citizen) as much as it is in the real world, perhaps more so. And although much can be gained from being online, much can be lost as well. It's important not to trust everything you read on the Internet and to take the trouble to find out about security, especially if you are going to conduct commerce online. Oh, and I was kidding about the tattoos on my feet.

Stay safe!

Additional Info

Some precautions suggested by the IC3 at http://www.ic3.gov/media/annualreport/2008_IC3Report.pdf with regard to Cyberstalking, although many of these precautions can be applied to general online safety.

“- Use a gender-neutral user name/e-mail address.

- Use a free e-mail account such as Hotmail (www.hotmail.com) or YAHOO! (www.yahoo.com) for newsgroups/ mailing lists, chat rooms, Instant messages (IMs), e-mails from strangers, message boards, filling out forms and other online activities.
- Don't give your primary e-mail address to anyone you do not know or trust.
- Instruct children to never give out their real name, age, address, or phone number over the Internet without your permission.
- Don't provide your credit card number or other information as proof of age to access or subscribe to a website you're not familiar with.
- Lurk on newsgroups, mailing lists, and chat rooms before “speaking” or posting messages.
- When you do participate online, be careful – only type what you would say to someone's face.
- Don't be so trusting online – don't reveal personal things about yourself until you really and truly know the other person.
- Your first instinct may be to defend yourself – Don't – this is how most online harassment situations begin.
- If it looks too good to be true – it is.”

Links and Resources

Take a look at <http://www.hotscams.com/> if you want to see just what kind of scams are being perpetrated on the Internet.

“Online Banking Fraud” by rander on www.therandtoday.com, 7 May 2008
<http://www.therandtoday.com/2008/05/07/online-banking-fraud/>

“Secure Your Identity in Online Business” by Rander on www.therandtoday.com, 25 January 2008
<http://www.therandtoday.com/2008/01/25/secure-your-identity-in-online-business/>

“Don't Blame Banks for Internet Fraud” by Heather D'Alton on iafrica.com, 24 July 2006
<http://personalfinance.iafrica.com/banking/708832.htm>

“Phishing Schemes Scar Victims” by Brian Krebs, Washington Post, November 18, 2004
<http://www.washingtonpost.com/ac2/wp-dyn/A59349-2004Nov18?language=printer>

“Bank Warns of Phishing Increase” from IOL (www.iol.co.za), March 26, 2007
http://www.iol.co.za/index.php?set_id=1&click_id=13&art_id=vn20070326172656442C278205

About The Author

Greg Bahlmann is a website designer and web developer based in Johannesburg, South Africa. He helps manage EZBIZsa web suites and is a keen supporter of promoting the Internet as a vehicle for small business proliferation.



Easy-to-use, inexpensive, full-featured small business web suites for only R269,00 per month (and a once-off R100,00 admin fee). Free .co.za domain name. We build your site for free - you just add content. No contract. 10 day money back guarantee. Loads of business functions and tools. Very, very easy to use. Professional support. Visit www.ezbizsa.com to find out more.

Distribution

Please feel free to distribute this document as by e-mail or as a download from your website or in any other way. However, please make sure that the content stays intact (in other words, no changes can be made) and if the information herein is used in any other format, credit is to be given as follows;

“by Greg Bahlmann (www.ezbizsa.com)”

Disclaimer

This article is intended to be informational in nature and the author makes no assurances as to the accuracy of information quoted herein. The author does not endorse any products or services mentioned above nor does he guarantee that following the advice of this article will prevent financial or any other kind of losses.