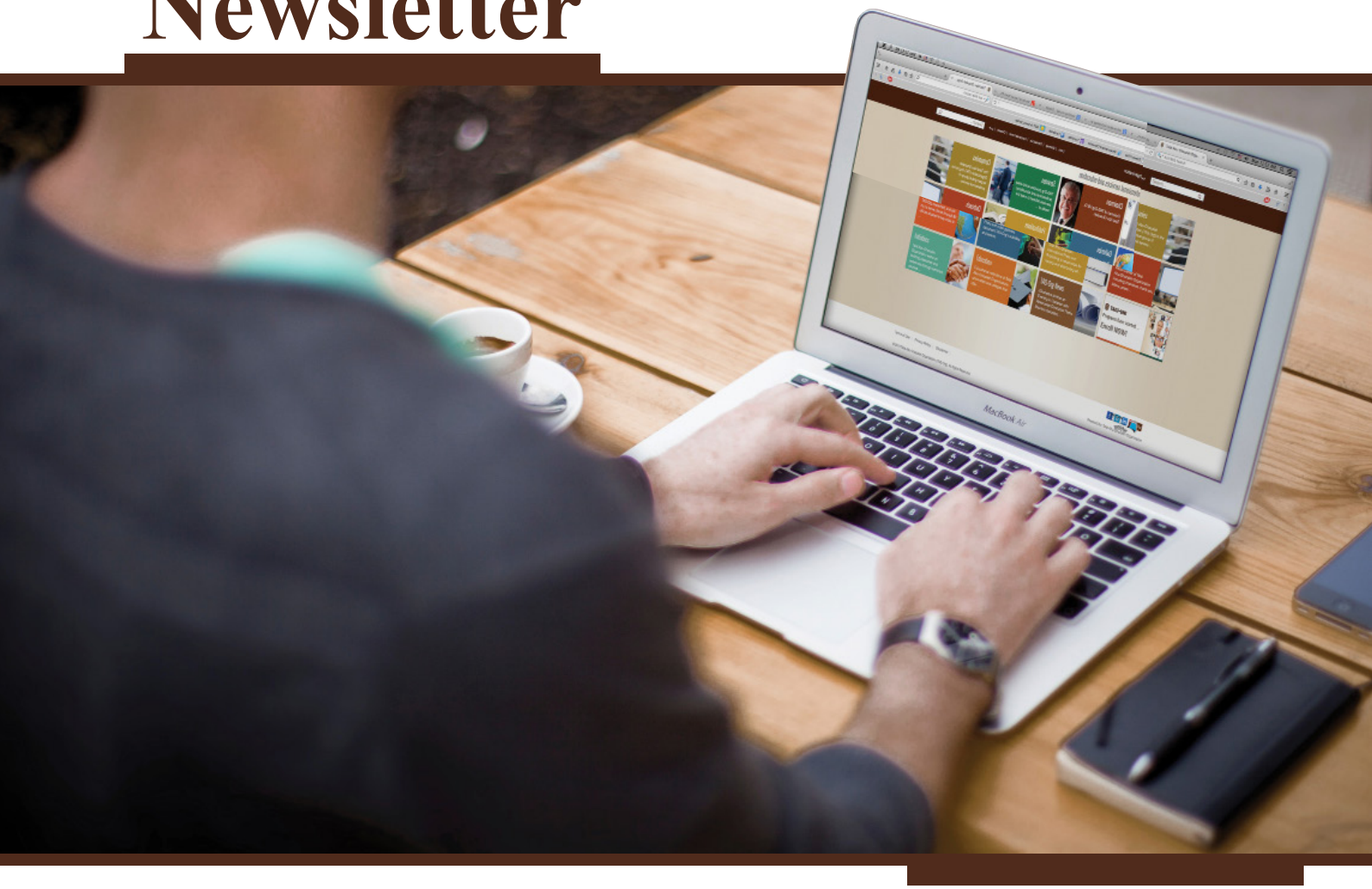
TAG-ITI

Talal Abu-Ghazaleh Information Technology International

Newsletter



OCTOBER 2018 | ISSUE 27

IN THIS ISSUE

TAGITI signs IT audit agreement with Rum Financial Brokerage

AMMAN- Talal Abu Ghazaleh Information Technology International (TAGITI) has signed an agreement with the Rum Brokerage to provide them with IT audit related services.

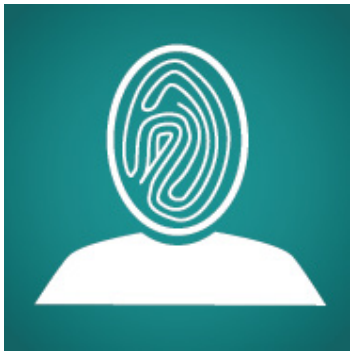
The scope of work will cover all of RUM's IT infrastructure and will help ensure that it is in line with Jordan Securities Commission IT audit program for financial brokerage firms.

Mr. Shahid Halling, TAGITI Support Director said that "Rum Brokerage has shown great confidence in our abilities to help them improve their IT practices and infrastructure. Our work will involve independently reviewing the IT controls they have in place and identifying areas of improvement in RUM's people, processes and technology."

He went onto say "Such work is extremely valuable and helps IT teams to independently identify threats their infrastructure is exposed to as well as providing regulatory authorities with the needed assurance that their IT infrastructure is up to standard."

http://tagiti.com/en/article/6684

How to protect your online identity



In just about every country around the world there are people who make a living stealing other people's identities. In fact, identity theft is one of the fastest growing crimes in the Arab region and stories of computer hacking, viruses and scams appear in the news almost daily. And while it may seem like something that only happens to other people, identity theft can affect anyone – including you.

The more you know about how it can happen, the easier it is to protect yourself.

What is identity theft?

Identity theft happens when someone uses your personal information without you knowing about it. And the risks can be significant. When you do things like log on to a website, enter a contest, sign up for a social network or pay bills through online banking, you're providing a wealth of information that can be stolen. That doesn't mean you shouldn't do these things – it just means you need to be smart and protect yourself.

Ways your ID can be stolen

As the saying goes, "Where there's a will, there's a way." And when an identity thief wants your information, they'll do everything they can to get it.

Here's how they do it:

- They pretend to be a reputable company and send fake emails and texts (phishing) or create fraudulent websites (spoofing) to trick you into providing personal and financial information.
- They scan old computers, servers, mobile devices, memory sticks or USB drives for information. When you get rid of or give away outdated equipment, make sure you delete all your personal information first by wiping it clean.
- They "shoulder surf" when you're using a public computer or your own computer in a public space. Anytime you log on to social networking sites, do your banking or surf in public – any time a password or personal information is required – be sure no one is looking over your shoulder.
- They will use "spyware", which is malware that is installed on computers to steal information about the user. It's most often found on public computers, but can also be installed on your personal PC or smartphone (via texts) without your knowledge through unsolicited emails or downloads.
- They will hack computer networks, systems and databases and find ways to divert your personal emails to them. Some individuals make a game out of this, and if they're successful, there's a risk of publicly exposing your personal information.
- They advertise jobs that don't exist to get you to submit your resume online.
- Some will use inside privileges in companies – such as an IT department that has access to employee information.

- They could use a brute-force attack to guess common passwords and try different combinations to crack yours.
- They browse social networking sites or dating sites looking for personal details. With low, open security settings, one doesn't have to "friend" you to gain access to potentially sensitive information which can be used to mount a personalized phishing attack against you or your friends.
- Remember, the offline world provides lots of opportunities for clever thieves who can then use your information both on and offline. To protect yourself out there in the 'real' world, here are some things that identity thieves will do to steal your personal information:
- They go through your mailbox or the recycling box you keep outside your home. Be sure to shred credit card bills - using a shredder - or other mail with your information on it.
- They get information from your wallet, purse, home, car, computer, or mobile device. Always check your locks on vehicles and keep things close to you when you're out and about or at work.
- They make telephone calls posing as someone they're not - such as a trusted official or law enforcement representative – and ask for your credit reports or bank account password. Also, a caller ID is no guarantee that the caller is from a particular organization as it can be spoofed.
- They tamper with ATMs and point of sale terminals and record your personal identification number (PIN). Or "shoulder surf" while you're using an ATM or paying at a store sales counter.

Clues that your ID is being used

Follow your instincts if something just doesn't seem right. There are a lot of signs that could indicate your personal information has been compromised.

For example:

- You don't recognize the purchases or withdrawals on your bills or statements.
- You're alerted by your bank or credit card company about suspicious transactions.
- Bills arrive for accounts you've never opened.
- Bills and bank or credit card statements arrive late or not at all (they may have been redirected).
- A creditor or collection agency contacts you about debts you weren't aware of.
- Your credit limit goes up without you requesting it (note that some financial institutions do this automatically).

What to do if identity theft happens to you

If for any reason you believe or suspect that your personal information may have been compromised, be sure to do the following as soon as possible:

- Call the police/national e-crimes unit and keep note of the report number for reference.

- Call your bank (look for the number on the back of your bank card).
- Call your credit card issuer (look for the number on the back of your credit card).
- Call credit agencies (companies that determine your credit rating) and put a fraud alert on your credit report:
- Keep records of all the steps you've taken (to clear your name and re-establish your credit).
- Look for numbers on printed statements (if you have lost your credit card, you don't have that as a source of information).

What happens after identity theft

Aside from the inconvenience of having to cancel and open new accounts, identity theft can lead to more serious consequences:

- Bills, charges, bad cheques, and taxes
- Clearing your name
- A damaged reputation if your name isn't cleared
- Bad credit rating, which could make finding employment or getting credit difficult
- Emotional issues from feeling violated and having to deal with the consequences

If you do have the misfortune of having your personal information compromised, the best thing you can do after addressing the immediate aftermath is to become as knowledgeable as you can about protecting yourself in the future.

Just as you wouldn't stop driving after a traffic accident, you can't be expected to stop using a computer if you become a victim of identity theft. But do ensure you take all the necessary precautions when you use your computer, phone or other devices going forward.

Online Identity Protection Tips

The easiest way to avoid identity theft? Don't let it happen. Keep these tips in mind at all times to help keep you safe:

- Before you share personal information, consider carefully what you're putting out there through email and social networking sites. This could include information like your cell number, address, hometown, workplace, status updates that let people know you're away and other revealing details.
- If you're asked for your personal information, find out how it will be used and why it's needed.
- Don't provide any more information than is required.
- Choose strong passwords. Don't use simple words or favorite names (like your child's name or your mother's maiden name). Try a combination of upper and lower case letters, numbers and symbols. You'd be surprised how many people use easy-to-crack passwords like '12345' or simply 'password'.
- Don't keep it in your wallet, saved on your computer or on your mobile device.
- Never use automatic login features that save your username and password. Take the time to re-enter your password each time.

- Don’t use your credit card number online unless you know the company you’re dealing with is reputable and the website is secure.
- If you use webmail, make sure you are using a secure connection, a feature available from all of the major services.
- Use “2-step verification” to log on to web services, if this feature is available. Services using 2-step verification first ask you for a password and then verify your identity through a separate channel such as by a text message on your phone.
- Do not reply to or click on links in any email that looks suspicious. Never open an attachment from spam or sender not known to you. Make sure that you are using anti-spyware software and that it is up-to-date.
- Always be wary of emails from financial institutions, Internet service providers and other organizations asking you to provide personal information online. If in doubt, call the company directly and ask them to verify the email.
- Only make online purchases from companies you trust.
- Clear your cache after banking or shopping online to make sure personal information isn’t stored on your computer. Here are examples of how to do this:
- In Firefox, go to Tools > Clear Recent History
- In Internet Explorer, Go to Tools > Delete Browsing History
- In Chrome, go to the wrench icon in the top right hand corner. Under the Bonnet > Clear Browsing Data
- Never leave your laptop in the car or anywhere else where it could easily be stolen.
- Make sure you have a firewall and that it’s set to “on”, install or upgrade virus protection software, and turn off file sharing to keep information on your computer safe. If you’re not sure how, you may want to ask a professional to do these things for you.
- Keep in mind that Wi-Fi networks in public places like coffee shops, libraries or airports are not secure. Never send personal information through public Wi-Fi and disable the connection when you’re not using it.
- Set up your home Wi-Fi network with an administrative password and other protective measures such as encryption. Avoid naming the network something identifiable to you – your phone number, address or family name.
- Before you sell or dispose of your computer or mobile device, completely wipe its hard drive to remove files, personal photos and all the information you have stored on it with overwrite software. You can buy overwrite software or have a professional do this for you. Even better, have the hard drive or device destroyed.

Source: https://www.getcybersafe.gc.ca/cnt/prtct-yrslf/prtctn-dntty/dntty-101-en.aspx
http://tagiti.com/en/article/6685

Keeping children safe online

It's a different world for children growing up today. From the minute they're born, they're exposed to a digital world that will inevitably be their way of life – where plans are made via social networking sites, conversations are had over chat and text, and movies, games, music and TV shows are streamed at any time over the Internet.

And while it's also a wonderful educational tool, it can be a place where tough lessons are learned if children have unlimited, unsupervised access to things they may not fully understand.

The following list can help you keep your children safe when they use social networking sites like Facebook and Twitter, as well as mobile devices:

- Make sure the protection features of websites and software your children use are activated. There are tools available through your Internet Service Provider (ISP) to help you manage your children's online experience (i.e. appropriate Websites, amount of time spent online, who can and cannot contact them). It might also include other security features, such as pop-up ad blockers.
- Get to know the online environments your children use and teach them how to deal with inappropriate material.
- Talk to them about the implications of posting inappropriate pictures, saying disparaging things about other people and anything else that could damage a reputation or ruin a friendship.
- Remind them that the Internet is a public space. Things they do and say now on social networking sites could have implications down the road when they're looking for summer employment (employers often search personal profiles for information about candidates).
- Stay in the know about the latest ways children are communicating and what they're up to when they're at friends' houses.
- Keep an eye on the sites they're visiting by keeping the computer in a common area like the kitchen.
- Talk to other parents about their children's online privileges and what works for them.
- Educate them about the risks of webcam use with people you or your children don't know. Video that's broadcast over the Internet is permanently out there and can be saved by anyone for later viewing or distribution. If your computer has been hacked, another user could remotely control your webcam, so if you have an external camera, unplug it or cover your camera when it's not in use.
- If your child is using live text and voice chats for online games, warn them not to give personal information to a stranger.
- Be careful about what you post about your children or activities related to them like the location of their school, or where you or they are volunteering.

Source: https://www.getcybersafe.gc.ca/cnt/prtct-yrslf/prtctn-fml/chld-sf-en.aspx
http://tagiti.com/en/article/6686

For More Information:

Talal Abu-Ghazaleh Information Technology International TAG-ITI

Tel: (0962-6) 5100900
Fax: (0962-6) 5100901

Or you may reach us electronically through our website:
TAGITI.com

And our email:
shalling@tagiti.com

This newsletter is published by:
Talal Abu-Ghazaleh Information Technology International (*TAG-ITI*)