Seed Weekly

Security Safeguards by Evan

There is no doubt that we have all be settling into a new way of doing since the Protection of Personal Information Act (POPIA) of 2013 came into full effect on 1 July 2021.

The Act states that a company must secure the integrity and confidentiality of personal information in its possession by taking appropriate, reasonable technical and organizational measures to prevent loss, damage or unlawful access to personal information. This means that you must have a reasonable amount of data security safeguards in place. Let's discuss a few of these security safeguards to ensure that your Advisory is up to speed.

Secure Your Server

Many companies run a server to save their files in a central location. To secure this server, at bare minimum, one needs a firewall, which is a system that monitors and controls incoming and outgoing network traffic based on predetermined security rules. In other words, it establishes a barrier between a trusted network and an untrusted network, such as the internet.

Remotely Access Your Server via A Virtual Private Network (VPN)

With the onslaught of Covid we experienced a shift from working in the office, to more employees working from home. This requires a Virtual Private Network (VPN) that can be accessed remotely and securely. Employees are able to connect to the server via VPN and make use of third-party software that enables multi factor authentication. When installed, it means that each time a user wants to connect to the server remotely, not only must the user enter their password, but also approve the login via their mobile phone.

Be Proactive About Keeping The Bad Guys Out

Understanding the potential risks is not always easy in an ever-changing environment, and a monthly server vulnerability scan will help you to identify these areas of concern. This is a process whereby white hat hackers (the good guys) probe your server from the outside and come up with a list of system vulnerabilities. This can then be put forth to your IT team to rectify and prohibit black hat hackers (the bad guys) from exploiting these vulnerabilities.

Seed Weekly

Security Safeguards by Evan

Implement An Internal Password Policy

Each employee has a desktop or laptop computer. This needs to connect to the company domain via a username and password. To safeguard against simple passwords, a business needs a password policy. The password policy deals with things like how often and when passwords should be updated, as well as a few minimum requirements. For example, your policy could state that a password must have a minimum length and some complexity requirements such as containing one capital letter and at least one number or character.

Install Anti-Virus Software – On Every Device

Every computer needs an anti-virus. This blocks potentially harmful programs from executing and disinfects and quarantines infected files. A good anti-virus updates regularly.

Encrypt Your Data

What happens to the data that is on a laptop in case of theft? If no safeguards are in place, the malicious thief can remove the hard drive, plug it into a new computer and access its contents. Fortunately, there is a thing called hard drive encryption. This is where one can password protect the contents of your hard drive. In this instance, even the removal of the hard drive, and plugging it into another computer, would still requires a password prior to accessing the contents.

Don't Overlook Your Emails

It is important to protect all your employee email boxes, not only from being accessed by a malicious party, but also against spoof emails, phishing emails and ransomware. To safeguard against unauthorized access, you can set up multi factor authentication so that user will need to confirm via their mobile phone when attempting to log into their email box. To safeguard against spam, viruses, phishing or spoofing emails, one can turn to solutions like Mimecast. Mimecast deletes these emails before they even reach your users. Providers of this nature are constantly evolving in order to identify the latest security threats.

These are just some of the data security safeguards that we employ at Seed Investments to help keep our valued data safe, and I am available to answer any questions that you might have in the process of keeping your Advisory data safe.

Kind regards,

Evan Smit *B.Com*
Business Analyst & Deputy Information Officer (POPIA)

Seed Weekly

Security Safeguards by Evan

DISCLAIMER

Seed Investment Consultants is an Authorised Financial Services Provider in terms of the Financial Advisory and Intermediary Services Act (Act No. 37 of 2002). The laws of the Republic of South Africa shall govern any claim relating to or arising from the contents of this document. This document may not be amended, reproduced, distributed or published without the prior consent of Seed Investment Consultants.

No guarantee is provided as to the values of any financial product mentioned in this document. All illustrations, forecasts, information and opinions provided within this document are of a general nature and are not intended to address the circumstances of any particular individual or entity. This document does not constitute a solicitation, invitation or investment recommendation. While we endeavour to provide accurate and timely information, all illustrations, forecasts or hypothetical data are not guaranteed and are provided for illustrative purposes only. We make no representation or warranty, expressed or implied with respect to the correctness, accuracy or completeness of the illustrations, forecasts, information or opinions. No party should act upon such information or opinion without obtaining the appropriate professional and specialised financial, legal and tax advice based upon a thorough examination of their particular situation. Seed Investment Consultants will not be held liable for any direct or consequential loss or damage suffered by any party as a result of that party acting on or failing to act on the basis of information or opinion provided by or omitted from this document.

The value of financial products can increase as well as decrease over time depending on the value of the underlying securities and market conditions. Changes in exchange rates may have an adverse effect on the value price or income of any product.

Past performance is not necessarily a guide to future performance. Performance has been calculated using net NAV to NAV numbers with income reinvested. The performance for each period shown reflects the return for investors who have been fully invested for that period. Individual investor performance may differ as a result of initial fees, the actual investment date, the date of reinvestments and dividend withholding tax. Full performance calculations are available from the manager upon request.

Prescient Management Company (RF) (Pty) Ltd are registered and approved under the Collective Investment Schemes Control Act (No.45 of 2002). Collective Investment Schemes in Securities (CIS) should be considered as medium to long-term investments. There is no guarantee in respect of capital or returns in a portfolio. CIS's are traded at the ruling price and can engage in scrip lending and borrowing. The CIS may borrow up to 10% of the market value of the portfolio to bridge insufficient liquidity. A CIS may be closed to new investors in order for it to be managed more efficiently in accordance with its mandate. CIS prices are calculated on a net asset basis, which is the total value of all the assets in the portfolio including any income accruals and less any permissible deductions (brokerage, STT, VAT, auditor's fees, bank charges, trustee and custodian fees and the annual management fee) from the portfolio divided by the number of participatory interests (units) in issue. Forward pricing is used. In the event that specific CIS in securities are mentioned please refer to the relevant Minimum Disclosure Document in order to obtain all the necessary information in regard to that unit trust. In rare instances redemption transactions may be subject to a redemption fee. The applicable Prospectus and Key Investor Information Document will be made available upon request.

Please note that there are stipulated cut-off times for all documents, notifications of deposit, investment, redemption and switch applications. These cut-off times are product or fund specific and the applicable guidelines have been stipulated on the relevant supporting or transaction documents, application forms and Minimum Disclosure Documents. Where all required and supporting documentation is not received before the stated cut off time no service provider shall not be obliged to transact at the net asset value price as agreed to. Prices are published daily and are available on the Prescient website at www.prescient.co.za.

Investors should at all times remain aware of the risks involved in the buying or selling of any financial product. Where foreign securities are included in a portfolio there may be potential constraints on liquidity and the repatriation of funds, macroeconomic risks, political risks, foreign exchange risks, tax risks, settlement risks, and potential limitations on the availability of market information. The investor hereby acknowledges the inherent risk associated with any selected investments and that there are no guarantees (Paragraph 6(2)(f) of BN92). The Manager retains full legal responsibility for any third-party named portfolio (Paragraph 6(1)(g) of BN92).

For any additional information please visit our website on **www.seedinvestments.co.za.**