BALLENTINE PARTNERS

Risk Management

How to Prevent Being Stolen From *Keeping the Crooks and Hackers at Bay*

BALLENTINE PARTNERS | SAM GOUGH, CPF® | MAY 2014

They are often very competent, clever, and persistent. Judging by the 70 million-plus credit card numbers they recently stole from Target, they can be quite ambitious, too.

They are the crooks and hackers who lift identities, clean out bank accounts, or simply empty wallets. And while everyone is on their radar screen, those with wealth stand out – not just for the size of their assets, but also for their vulnerability.

The good news is there is a lot you can do to protect yourself and your family. It won't take that much time – most of the effort involves simple, common-sense steps – and the return on this investment, in terms of increased security and peace of mind, will be huge. To be sure, no protection plan is foolproof, so we'll also discuss some tips to limit the damage should a breach occur.

The two biggest security threats that you face are close at hand: your personal computer and your household staff. The information that is stored on your laptop and other electronic devices often tell your entire financial life story, and it's there for the taking. Meanwhile, many trusted employees are given access, asked to pay bills, handle bank accounts, and use credit cards on behalf of the families they serve.

Safer Driving on the Electronic Highway

An electronic thief sometimes needs no more than your email address to get started – and there are many ways to get that. They would also like to get your user name and password for your computer and sensitive accounts. (The New York Times recently reported, for example, that one of the Internet's key security methods had a flaw that could potentially expose user names and passwords at many highly popular websites.)

If a thief gains access to your computer, there is plenty to explore, from financial statements and credit card bills to tax returns and email correspondence with accountants, lawyers, and financial advisers.

To ward off an attack or limit your vulnerability, consider the following:

- Don't help the bad guys. Hackers often come "phishing" for more information, sending an email that purports to be from your bank or broker, say, and asking you to supply sensitive information or click on a link to a "company" site, a move that could well unleash a nasty virus. Be rude and don't respond.

- Double down on authentication. You're feeling pretty safe because you change your password on a regular basis. Unfortunately, that's not enough. Up-to-date hackers have cutting-edge tools, and if they already possess some of your credentials, they probably can get the rest. For instance, they can use computer firepower, in the form of a so-called brute force attack, to go through endless random guesses to crack a password lickety-split. You will make the task much harder for them by opting to use "two-factor authentication" for any online accounts or logins that offer it. Enabling this feature essentially adds another wall of protection, requiring a separate access code after the password is entered – a code that changes every few seconds. You shouldn't have a problem getting in because the code is transmitted directly to your phone or electronic device. But if someone tries to log into your account without the access code, in most cases the system will not only keep them out but it will also alert you to the attempted breach.

- Install really good defensive software. Include anti-virus protection and a personal firewall. And keep it up to date.

- Operate using the least privileges possible. Create a user login as well as an administrator login. As a user, you will be able to access the programs on your computer but will need to input the administrator password in order to download programs or make changes to the device. If you operate as the administrator and your computer is compromised, the hacker will then have administrative privileges.

- Thin out those sensitive files. Don't use your email box as a repository for your financial and other personal records. Download them to an external hard drive or memory sticks.

- Be wary of going online in public places. Airports, hotels, coffee shops and other public venues offer easy access to the Internet, but their networks are usually unsecured. That makes you particularly vulnerable to malware. If such malicious software is loaded into any computer attached to the network, it can spread to any other unprotected computer that is also attached, contaminating it and grabbing valuable information. The safer way to connect when traveling is to use your own portable – and secured -- broadband modem.

- Travel light when going abroad. Bring a "clean" phone and laptop, empty of all sensitive files and information. In certain countries, security is largely unobtainable.

Should an attack succeed, speed is of the essence in limiting the damage.

- Spread the word. Notify everyone – from financial institutions to retailers – with whom you have an account. But don't sound the alarm via email – the hacker may still be on the job and could block such a message from reaching its intended recipient. Instead, use the phone.

- Change your email credentials. That might even mean going to a new platform. And once you make the change, spread that news as well – since you are now safe, you can use email for this message.

- Consider bringing in a professional. If your computer is compromised by a virus, you will likely need to bring in a professional to completely clean your devices. If your device is hacked, setting up a new email address will not be enough as the hacker will have access to your new email credentials.

- Hackers often contact a bank or financial adviser posing as the person they have just hacked.

Using the victim's email address, or a fake email address that is almost identical to the victim's real one, off by perhaps just a single character, they try to make arrangements to transfer funds, often by mimicking conversations they have read in the hacked emails.

- Because we work so closely with our clients over such lengthy periods of time, we recognize behavior that is out of the ordinary and are not easily fooled by such requests. In fact, we are sometimes the first to realize that a breach has occurred and we react immediately to limit the damage – among other things, by putting stop orders and alerts on all of the affected client's accounts. We are happy to say that in many cases there is no damage at all, other than a heightened sense of vulnerability.

Less Worry at Home

By definition, you trust your household staff -- after all, they may be balancing your checkbooks and paying your bills. In fact, over the years, you may have gotten close enough to some members of the staff to think of them as family.

Yet, in too many cases, the trust is misplaced. To be prudent, a number of safeguards are needed, not only to protect you and your family but also to protect the staff, sometimes from their temptation and sometimes from your misguided suspicion.

Put things away. Anyone who has access to your house – regular staff, fill-ins or even repairmen and delivery people -- may use it to get copies of checks and other sensitive documents. All it takes is a snapshot from a smart phone. So keep all of these papers in a locked cabinet or desk, and make them available only to the person who works with them on a regular basis.

Stay engaged. Don't delegate too much. Make sure that you receive bank statements, credit card bills and other financial reports in their sealed envelopes and examine them closely before handing them over to the staff for processing and payment. Also review the copies of cancelled checks.

Keep control of the final payment step. We strongly recommend that you remain the one who must authorize payment of all bills. It's easy to do online. Banks typically have software that allows different levels of access during the payment process – one person prepares the payments but a second person reviews and authorizes payment, either for a whole batch of bills or one by one.

Tighten up the credit strings. Put a monitoring system in place that bars the opening of any new credit account without a phone call to you.

Be realistic about trust. Blind trust may hurt you. We suspected a household employee of stealing and raised that possibility with the client. The client had met the employee under circumstances that caused the client to feel a strong bond with the employee. Although the evidence linking the employee to thefts continued to mount, the client resisted considering that possibility. It took us three years, and many heated discussions, to get the client to recognize the situation and agree to act. Conversely, it is just as important not to unfairly accuse a staff member of doing something wrong. To keep that from happening, it is essential to build a system around each of your staff, adopting the steps outlined above, that diminishes the risk of a breach and of a false accusation. Staff who truly are trustworthy should be willing to support a system of checks and balances that are designed to insure that unauthorized transactions are extremely unlikely to occur. A trustworthy staff member will have a strong desire to make sure that if something goes wrong, he or she will not be under suspicion.

Conclusion

Wealth confers many privileges, not least a buffer against some of life's vicissitudes. But in the case of hackers and other crooks, it does the opposite. For them, the wealthy are not random targets. The electronic bad guys even use algorithms to search them out.

With this in mind, it makes sense to build your own buffer. It won't take long, and the dividends may go on forever.

About Sam Gough, CFP®

Sam is a Wealth Planner and his area of expertise is implementing clients' complex estate planning and investment strategies. Sam serves as a specialized resource for his clients, whose families often have extensive financial infrastructure including multiple family investment and charitable entities. In addition, Sam runs our Risk Management Knowledge Management team, which focuses on the advice and ideas we deliver to clients about how to manage and mitigate risks across their financial lives.

BALLENTINE
PARTNERS

info@ballentinepartners.com
https://ballentinepartners.com