ALERT TO ALL SHERIFFS

CYBER CRIME

ISSUED : MARCH 2020, 19

The South African Board For Sheriffs would like to alert the sheriffs' profession about the increasing levels of e-mail frauds and the fact that cybercrime is not covered by the policy provided by the Professional Indemnity Insurance Fund.

Introduction

Cybercrime, also called **computer crime**, the use of a computer as an instrument to further illegal ends, such as committing fraud, trafficking in child pornography and intellectual property, stealing identities, or violating privacy. Cybercrime, especially through the Internet, has grown in importance as the computer has become central to commerce, entertainment, and government.

Although the attacks do not take place on a physical body, they do take place on the personal or corporate virtual body, which is the set of informational attributes that define people and institutions on the Internet. In other words, in the digital age our virtual identities are essential elements of everyday life: we are a bundle of numbers and identifiers in multiple computer databases owned by governments and corporations. Cybercrime highlights the centrality of networked computers in our lives, as well as the fragility of such seemingly solid facts as individual identity. cybercrime of one sort or another.

Types of cybercrime

Cybercrime ranges across a spectrum of activities. At one end are crimes that involve fundamental breaches of personal or corporate privacy, such as assaults on the integrity of information held in digital depositories and the use of illegally obtained digital information to blackmail a firm or individual. Also at this end of the spectrum is the growing crime of identity theft. Midway along the spectrum lie transaction-based crimes such as **fraud, trafficking in child pornography, digital piracy, money laundering, and**

counterfeiting. These are specific crimes with specific victims, but the criminal hides in the relative anonymity provided by the Internet. Another part of this type of crime involves individuals within corporations or government bureaucracies' deliberately altering data for either profit or political objectives. At the other end of the spectrum are those crimes that involve attempts to disrupt the actual workings of the Internet. These range from spam, hacking, and denial of service attacks against specific sites to acts of cyberterrorism—that is, the use of the Internet to cause public disturbances and even death. **Cyberterrorism** focuses upon the use of the Internet by nonstate actors to affect a nation's economic and technological infrastructure. Since the September 11 attacks of 2001, public awareness of the threat of cyberterrorism has grown dramatically.

Identity theft and invasion of privacy

Cybercrime affects both a virtual and a real body, but the effects upon each are different. This phenomenon is clearest in the case of identity theft. In the United States, for example, individuals do not have an official identity card but a Social Security number that has long served as a de facto identification number. Taxes are collected on the basis of each citizen's Social Security number, and many private institutions use the number to keep track of their employees, students, and patients. Access to an individual's Social Security number affords the opportunity to gather all the documents related to that person's citizenship—i.e., to steal his identity. Even stolen credit card information can be used to **reconstruct an individual's identity**. When criminals steal a firm's credit card records, they produce two distinct effects. First, they make off with digital information about individuals that is useful in many ways. **For example, they might use the credit card information to run up huge bills, forcing the credit card firms to suffer large losses**, or they might sell the information to others who can use it in a similar fashion. Second, they might use individual credit card names and numbers to create new identities for other criminals.

For example, a criminal might contact the issuing bank of a stolen credit card and change the mailing address on the account. Next, the criminal may get a passport or driver's license with his own picture but with the victim's name. With a driver's license, the criminal can easily acquire a new Social Security card; it is then possible to open bank accounts and receive loans—all with the victim's credit record and background. The original cardholder might remain unaware of this until the debt is so great that the bank contacts the account holder. Only then does the identity theft become visible.

Internet fraud

Schemes to defraud consumers abound on the Internet. Among the most famous is the Nigerian, or "419," scam; the number is a reference to the section of Nigerian law that the scam violates. Although this con has been used with both fax and traditional mail, it has been given new life by the Internet. In the scheme, an individual receives an e-mail asserting that the sender requires help in transferring a large sum of money out of Nigeria or another distant country. Usually, this money is in the form of an asset that is going to be sold, such as oil, or a large amount of cash that requires "laundering" to conceal its source; the variations are endless, and new specifics are constantly being developed. The message asks the recipient to cover

some cost of moving the funds out of the country in return for receiving a much larger sum of money in the near future. Should the recipient respond with a check or money order, he is told that complications have developed; more money is required. Over time, victims can lose thousands of dollars that are utterly unrecoverable.

The victim **willingly provides private information** that enables the crime; hence, these are transactional crimes. Few people would believe someone who walked up to them on the street and promised them easy riches; however, receiving an unsolicited e-mail or visiting a random Web page is sufficiently different that many people easily open their wallets. Despite a vast amount of consumer education, Internet fraud remains a growth industry for criminals and prosecutors. Europe and the United States are far from the only sites of cybercrime.

ATM fraud

Computers also make more mundane types of fraud possible. Take the automated teller machine (ATM) through which many people now get cash. In order to access an account, a user supplies a card and personal identification number (PIN). Criminals have developed means to **intercept both the data on the card's magnetic strip as well as the user's PIN.** In turn, the information is used to create fake cards that are then used to withdraw funds from the unsuspecting individual's account. A particularly effective form of fraud has involved the use of ATMs in shopping centres and convenience stores. These machines are free-standing and not physically part of a bank. Criminals can easily set up a machine that looks like a legitimate machine; instead of dispensing money, however, the machine gathers information on users and only tells them that the machine is out of order after they have typed in their PINs. Given that ATMs are the preferred method for dispensing currency all over the world, ATM fraud has become an international problem.

Wire fraud

The international nature of cybercrime is particularly evident with wire fraud. One of the largest and best-organized wire fraud schemes was orchestrated by Vladimir Levin, a Russian programmer with a computer software firm in St. Petersburg. In 1994, with the aid of dozens of confederates, Levin began transferring some $10 million from subsidiaries of Citibank, N.A., in Argentina and Indonesia to bank accounts in San Francisco, Tel Aviv, Amsterdam, Germany, and Finland. According to Citibank, all but $400,000 was eventually recovered as Levin's accomplices attempted to withdraw the funds. Levin himself was arrested in 1995 while in transit through London's Heathrow Airport (at the time, Russia had no extradition treaty for cybercrime). In 1998 Levin was finally extradited to the United States, where he was sentenced to three years in jail and ordered to reimburse Citibank $240,015. Exactly how Levin obtained the necessary account names and passwords has never been disclosed, but no Citibank employee has ever been charged in connection with the case. Because a sense of security and privacy are paramount to financial institutions, the exact extent of wire fraud is difficult to ascertain. In the early 21st century, wire fraud remained a worldwide problem.

The new wave of financial fraud

The South African Board For Sheriffs would like to alert the sheriffs' profession about the increasing levels of e-mail frauds and the fact that cybercrime is not covered by the policy provided by the Professional Indemnity Insurance Fund. Sheriffs operating trust accounts and who don't have the security measures in place to protect their confidential information are potentially at greater risk, not only on trust accounts but on their business accounts which are receiving trust funds.

Fraudsters no longer need access to your bank accounts in order to steal money. By hacking into your email, scammers can intercept invoices, changing the payment details of individuals and businesses.

What's happening?

Fraudsters are using phishing emails to **steal usernames and passwords**, allowing them to hack your personal or business or trust email accounts.

They then **troll and monitor your email account** for an opportunity to intercept an invoice. For example, when you are purchasing goods and awaiting an invoice on email, or if your business is sending an invoice by email.

The scammers **intercept an email, change the bank details on the invoice** and send it on for payment. In many cases, they use spoofing to make the email address seem credible and trustworthy. Spoofing changes a letter or domain in the email address to make it **appear legitimate**.

The recipient pays the invoice thinking it comes from a legitimate source, when in fact the money is paid into the scammer's account.

How does email payment fraud happen?

Email payment fraud occurs when a fraudster hacks into the email communications between a client and a company. The scammer places malware into a computer which will lie dormant until it recognises specific keywords relating to a request for funds or deposit payment. This is the stage that fraudsters make their move. They'll then contact the client, disguised as the attorney, informing them that the company's bank details have changed and requesting that they transfer the funds into the 'new' account. Fraudsters are now targeting sheriffs. Fraudsters are listening to emails and building up a timeline of the sheriff's transactions. After some time into the transaction, they'll contact the sheriff by email asking sheriffs to

transfer the proceeds of the sale. As they've been intercepting the emails, they'll be aware of the template and be able to produce an authentic-looking email. The fraudsters will then quickly withdraw the money, usually sending it overseas.

What should I look out for?

An attorney will not send you a last-minute email telling you that bank account details have changed; this should be your first warning sign.

How can I protect myself?

Be wary of any emails discussing payment details, and to double check its legitimacy before sending payment. Always confirm any requests directly, ideally in person or by the telephone, to ensure the instruction is genuine.

Use existing contact details

When you're contacting the company you're making the payment to, don't use the contact details from the email you've just received. If the email is fraudulent, then the contact details are likely to be false, too.

All sheriffs are reminded of their obligations to keep clients' money safe through appropriate systems. However, working practices will vary from office to office.

What are the consequences for sheriffs?

This type of fraud can lead to strained business relationships as neither party feels that they are responsible for the fraud. It can also lead to a loss of funds and may take a long time to sort out if there are legal implications.

This scam is prevalent in the conveyancing space. If you are a conveyancer, a sheriff or an estate agent, take extra precautions.

How to protect yourself

Here are some tips to help you prevent this fraud:

- You as a sheriff, handling large sums of monies, especially in trust, can pre-empt this type of attack. Let current and new clients know that your banking details will never change. If they receive any correspondence announcing a change in bank details, advise clients to contact you and verify your banking details before they pay
- You can also consider leaving your bank details off your invoices and call clients to give them this information instead.
- If you are an individual who is supplying banking details, do not email invoices with bank details. Instead, give your banking information directly over the telephone.
- stop using email technology to send sensitive documents like invoices to your clients. Secure file sharing platforms like YDOX, enables you to send and receive sensitive files in a secure environment where criminals cannot gain access to it.

Sheriffs operating trust accounts and who don't have the security measures in place to protect their confidential information are potentially at greater risk, not only on trust accounts but on their business accounts which are receiving trust funds.

This follows a judgment that was recently granted against a firm whose e-mail account was been hacked, resulting in them paying R1,7 million rand to a third party, and not to the person entitled to the money. The court held that the firm had a duty to verify that the e-mail giving instructions in regard to the payment indeed came from its client.

It is therefore not enough to assume that because an e-mail appears to come from a client, and that because the client's email address or their name appears on the mail, the e-mail does in fact come from that client. Sheriffs are advised to be careful when instructions are received with new bank account details, or an instruction is received to change the bank account details of a client or third party to whom funds are due. All such details **should be verified** by **telephone** or any other means. All sheriffs have an ethical duty to put appropriate systems in place to safeguard all their confidential information, failing which they may be viewed as being unprofessional and/or negligent.