Case studies

Case studies

Information security and cybercrime

Information security and cybercrime

Updated 25 November 2019 (Date first published: 24 July 2015)

Print this page [#] Save as PDF [https://higher-rights.sra.org.uk/pdfcentre/?type=Id&data=547408254]

Related resource

Examples below should be read in conjuction with our Risk Outlook [https://higher-rights.sra.org.uk/archive/risk/outlook/risk-outlook-2020-21/information-and-cyber-security/]
.

Example 1

Solicitor loses firm money by clicking on email attachment

The following case illustrates the importance of treating email attachments with caution, and independently verifying calls claiming to be from your bank.

A lawyer based in the US received an email appearing to be from a genuine sender. She clicked on an attachment in the email.

The next day, she tried to access the firm's office account online. The log in process seemed different, but she proceeded anyway.

The log in was rejected. Almost immediately she received a call from someone claiming to work for the bank, offering help. The person said the bank had noticed she was having difficulty logging in. The lawyer was asked to enter her username and certain characters of her PIN and password. After several attempts, the caller advised the account had been locked temporarily.

Three days later, the same person called again to offer help, this time with the client account. At this point, the lawyer became suspicious. She hung up the phone, checked for a dial tone, and placed a call to the bank using a known number.

The bank denied contacting her recently. Further enquiries revealed that the majority of the office account's balance had been transferred abroad to an overseas bank.

The bank told her it would be unable to retrieve the funds or accept liability as she had failed to safeguard the firm's online log in details. The firm was left to bear the loss.

The lawyer reported the fraud to the police. An expert said that by clicking on the email attachment, she had probably inadvertently downloaded a virus that detects attempts to connect to bank websites, and redirects the user to a fake version run by the hackers. The first attempt to log in would have provided the hackers with her username and some characters of her PIN and password. The perfectly timed phone call and subsequent attempts would have given the hackers the remaining characters.

Example 2

Law firm successfully withstands sophisticated cyber attack

The following case illustrates how having a secure backup of computer files can help firms counter a sophisticated cyber attack.

When the employees of a law firm arrived at work one day, they turned on their computers and found their desktop wallpaper replaced with a message. It warned that all the firm's office and client files had been encrypted. This meant the contents of the files had been scrambled, so anyone viewing the files would be unable to make sense of them. To regain access, the firm would need a password from the hackers.

The notice told the firm it had two days to pay a ransom. If it failed to pay, the hackers would delete the password and the firm would lose their files forever. It also said the encryption was unbreakable without the password.

The software used for this attack, known as Cryptowall ransomware, affected all three branch offices of the firm as they used a central network.

The firm reported the incident to the Information Commissioners Office and to the police, who said it was likely the attack came through either a malicious email attachment or by visiting a hacked website. Viruses on hacked websites can infect computers whose browsers have not been updated to withstand known threats, or do not have effective antivirus systems.

Fortunately the firm had a secure backup of all of its files, stored separately to its central network. As such, it refused to pay the ransom and the only loss was the time spent in reinstalling its files.

Example 3

Fraudsters instruct solicitor by pretending to be the client

The following case illustrates the importance of maintaining secure systems, and the harm that can arise to clients if firms fail to do this.

Miss A was acting for a client in the sale of a property. On the day the proceeds of the sale were to be paid into the firm's client account, Miss A received a message from her client's email address. It contained instructions to transfer the funds to the client after receipt, including details of a bank account in the client's name.

After the funds cleared into the firm's client account, Miss A transferred the funds as instructed.

The next day, the client called Miss A to ask whether the firm had received the proceeds from the sale. Miss A replied that the funds had been transferred to the client's personal account, as instructed in the email. However, the client denied emailing instructions to Miss A. They both contacted the bank the funds were sent to, only to be told the funds had subsequently been transferred abroad.

It appeared from the firm's investigation that a fraudster had hacked into the client's email account and sent the instructions to Miss A, under the guise of being the actual client.

This was a sophisticated fraud which would have required knowledge of the identity of Miss A's client, the type of matter Miss A was dealing with, and the stage the matter was in. The fraudsters may have obtained this information by using malicious software that allowed them access to the firm's systems.

The firm reported the matter to us and we are currently looking into it.

Example 4

Social engineering causes law firm to lose office money

The following case illustrates the operation of a financial fraud

Mr A was the managing partner of a medium sized law firm. One day, he received a telephone call from Ms B, who introduced herself as the new account manager for one of the firm’s suppliers. Ms B followed up the call a few days later in writing. She confirmed what they had discussed and informed Mr A of a change of payment details for future monthly payments, the first of which was due shortly.

Two weeks after making the payment, Mr A was contacted by a representative from the supplier enquiring why they had not been paid.

Ms B had been a fraudster, and had previously hacked into the supplier's email system to obtain details of their customers. Mr A's firm was just one of many that had been targeted in the same manner. The payment could not be recovered, leaving the firm with a financial loss.

To reduce the chance of this happening again, the firm instituted a policy of confirming requests to change bank account details by means of a telephone call to a known number.

Example 5

Fraudsters intercept solicitor-client emails to steal money

The following case illustrates why firms and clients should consider following up on unusual communications, using independent and established means.

Mrs A was being advised by XYZ Solicitors in the purchase of a buy-to-let property.

The day before she was due to send the purchase money to the solicitors, Mrs A emailed them to confirm details of the firm's bank account. She received two replies, both seemingly from her solicitor.

The first email contained the correct bank details. The second email, received minutes later, contained details of an account in the name of XYZ Solicitors but with a different bank. The email explained that the firm was having issues with their usual bank, and asked Mrs A to use their alternate account. This email was sent by fraudsters.

Mrs A called her bank and arranged for the funds to be transferred within 24 hours. She emailed the law firm to confirm this. This email, along with others sent by Mrs A and her solicitors, were deleted to prevent detection. The fraudsters also sent emails to both parties, assuring them everything was fine.

Three days elapsed, during which time the fraudsters transferred the money abroad.

They did this through several smaller transfers to avoid questions from their bank.

The fraud came to light only when XYZ Solicitors called Mrs A to find out what was happening. By the time the fraudsters' banking provider was alerted, all the money was gone. Mrs A's bank refused to refund her as they had acted on her instructions, leaving her to bear the loss.

It emerged that the fraudsters had hacked into the firm's email server, possibly by taking advantage of an outdated antivirus, internet browser or operating system.

They had used a bank account in the name of the law firm to make the fraud appear legitimate.

Example 6

Non-solicitor employee impersonates solicitor

The following case illustrates that fraudsters are not always faceless individuals – they can be people you know.

Mr Z was a sole practitioner in Z Solicitors, based in Bristol. He specialised in personal injury, and employed a non-solicitor to handle all administrative tasks.

We received two reports, within the space of a week, indicating that an individual was pretending to be a solicitor by using Mr Z's identity. Both reports referred to a Mr Z of Z Solicitors Ltd, based in Liverpool.

The first report was made by a member of the public after receiving a claim notification form, supposedly from Mr Z. When the individual visited the Liverpool address on the letter, he discovered the office was boarded up and had evidently not been in use for some time. We had no record of a Mr Z working from this Liverpool address. As a result, a scam alert was released on our website.

The second report was from a solicitor, after receiving correspondence from Z Solicitors Ltd. As the solicitor had never worked with Z Solicitors before, she performed due diligence checks and found the scam alert. This prompted her to make the report.

Our investigation revealed that Mr Z's administrative officer had deliberately entered false firm name and address details into several files on the case management system. She had done this to intercept payments to personal injury claimants.

We reported the administrative officer to the police for fraud and banned her from working in solicitors' firms.

Example 7

Fraudsters hijack firm's telephone line to cash fake cheques

The following case illustrates how law firms can be targeted to facilitate fraud, sometimes without their knowledge and through no fault of their own.

A law firm contacted us to report a fraud.

The firm's telephone line had been out of order on the previous Friday. When a partner of the firm dialled the number, it was answered by someone who claimed to be from their telecommunications provider. He said he was correcting a fault with the connection.

The following Monday, the firm received a call from a cheque cashing company. They advised they had called on Friday after a customer brought in two large cheques, seemingly issued by the firm. They had spoken with a Mr Z, who had said the cheques were genuine. As a result, the company had paid cash to the bearer.

The firm advised they had never heard of Mr Z, and that their telephone line was out of order at the time.

Minutes later, a client called to ask if the firm had received the money she had sent on Friday for a house purchase, after ringing to obtain their bank details. The firm had not.

The following investigations revealed the firm had been targeted by fraudsters. The fraudsters had contacted the firm's telephone company and convinced them to divert all calls to a number they were operating. They then presented fraudulent cheques in the name of the law firm. When the cheque cashing company had telephoned the firm to ask whether the cheques were genuine, the fraudsters had answered and said they were.

The fraud was reported to the police, who advised that the fraud could have been detected earlier if the firm had called their telephone company using an established number. It is not known at this stage whether the victims will be able to recover their money.

Example 8

Fraudsters hijack law firm's invoices

The following case illustrates how maintaining an up to date computer system, with antivirus software, can help protect firms against fraud.

A medium-sized law firm, XYZ Solicitors, sent invoices to nine clients by email. The firm provided details of their client bank account and asked for the payment to be made within four weeks.

Two weeks went by, but the firm failed to receive any payment. The practice manager, Mrs A, called one of the clients to make enquiries. The client said he had made the payment immediately after receiving the invoice, using the bank details provided on the invoice.

Mrs A obtained the details from the client and checked them against a bank statement. They did not match. However, the account the client had made the payment to was in the name of XYZ Law, which was similar to their own.

Mrs A subsequently called the other eight clients and found they had also paid into XYZ Law's account. When Mrs A called our Contact Centre to ask about the firm, she was told that it didn't exist.

The following investigations indicated that fraudsters had hacked into the firm's email server, intercepted the emails, and replaced the attached invoices with fraudulent ones containing different bank details. The fraudsters had deliberately used a bank account in a name similar to that of the law firm to make the fraudulent invoices appear legitimate. By the time XYZ Solicitors became aware of the fraud, the fraudsters had already transferred the money abroad.

The firm later consulted an IT security expert who advised that using an up to date antivirus, internet browser and operating system may have prevented the fraud.