WHAT'S INSIDE?

- 5 Common Fraud Schemes to know in 2021
- Watch out for these top internet scams
- Investigator of the month: Chris Porter - Polygraphs
- Ferlio Notification Board
- Specialist Services Offered
- Contact Us

Ferlio Group of Investigators

0860 337 546 / 0860 (F-E-R-L-I-O)

NEWSLETTER

Volume 02 – January 2021

As we enter into a new year, it is important to plan for the months ahead of us. Preparing your personal life as well as your business for potential risks is as important as ensuring you have sufficient stationary or if your budget is in order.

In this newsletter, we discuss the fraud schemes that one should be aware of as we enter the new year, top internet scams, as well as delve into cryptocurrency fraud

5 COMMON FRAUD SCHEMES TO KNOW IN 2021

BY ECONSUMER SERVICES

https://econsumerservices.com/5-common-fraud-schemes-2021/

2021 holds a lot of potential...but it could also bring new threats. Some trends in online fraud, for instance, are going to stick around and get even more pronounced in the new year. You've got to be prepared for what's going to come, and learn how best to protect yourself.

With all that in mind, let's take a look at some of the top fraud trends you need to know about heading into 2021.

#1. Authorized Push Payment Fraud

Credit rating agency Experian identified authorized push payment fraud (also known as "APP fraud" or simply "wire fraud") as the top threat encountered by businesses in 2020. This scheme is expected to remain in that top tier of fraud threats in 2021 as well.

APP occurs when fraudsters trick their victims into authorizing payments from their own account into another account controlled by a criminal. These fraudsters can intercept messages, even alter consumers' information, or even make up fake personas entirely. The goal for the fraudster is to trick their victims into authorizing payments to an account controlled by the fraudster.

APP fraud can be prevented by financial institutions that use real-time checks as a validation exercise. However, it's also up to consumers to verify identities before sending money to anyone.

In remembrance of George William Barnes (1954-2020)

#2. Account Takeover

With these incidents, a fraudster manages to hack into a user's account, then impersonate that customer. Criminals can do this as part of a phishing scheme, or the criminal might use some other means to find out your information. In either case, once the fraudster has access to your account, they are able to conduct transactions and other activity on your behalf.

One way to protect yourself here is to use two-factor authentication (2FA) when available. This means using a strong and secure password on all accounts, along with some other form of identification. Biometrics, for example, are a great option when available. Payment tools like Apple Pay and Samsung Pay allow you to require a biometric signature, like a thumbprint, to authorize purchases.

#3. New Account Fraud

This scheme, a form of identity fraud, occurs when criminals use stolen information to create a new account. The fraudster may impersonate a real person using information acquired through phishing or through some other method of hacking a user's data.

With the new account, fraudsters are able to take out lines of credit, make purchases, and conduct other business using a stolen identity (or multiple identities). This is not a new tactic; however, we anticipate that it will continue to grow rapidly as more consumers make purchases and do other business online.

You can defend against this tactic by keeping your information secure. Again, we recommend using strong, secure, and unique passwords for all your accounts. Also, educate yourself about the risk posed by phishing tactics.

#4. Synthetic Identity Fraud

Unlike other tactics, which involve a fraudster impersonating a real person, synthetic identity fraud occurs when a criminal uses different pieces of information to create a fake identity. This fake person can have a Social Security number from one individual, a name and date of birth from another, and billing information from another.

This is an advanced and complex threat, and it continues to be more of a problem with each passing year. When well-executed, it's extremely difficult for businesses to identify these schemes, which will only make them more popular over time.

While the use of the data is different, the tactics used to steal the data are no different from any other identity theft. Like account takeover or new account fraud, you can protect against synthetic identity fraud by ensuring that you stick to best practices to avoid phishing and other similar schemes.

#5. Friendly Fraud

Unlike other tactics, friendly fraud is perpetrated by cardholders, rather than against them. This scheme refers to abuse—either deliberate or accidental—of the chargeback process.

Chargebacks are an important form of consumer protection. They allow buyers to claw back their funds in the event of fraud. However, more and more cardholders are using them as a tool to effectively "get something for free." This has consequences for businesses, but it can negatively affect cardholders, too. If you get caught requesting unjustified chargebacks, it could result in penalties from your bank. They could even cancel your account, which may negatively affect your credit score.

If you believe someone made an unauthorized purchase on your account: don't panic. Be sure you investigate the situation fully. You don't want to file a chargeback on a transaction you authorized, then forgot about, or don't recognize at first glance.

In remembrance of George William Barnes
(1954-2020)

WATCH OUT FOR THESE TOP INTERNET SCAMS

BY ALISON L DEUTSCH

https://www.investopedia.com/articles/personal-finance/040115/watch-out-these-top-internet-scams.asp

Internet scams are continually evolving. The FBI documented a record $3.5 billion in losses due to internet crimes in 2019.1 Right now, con artists around the world are likely targeting a computer or mobile device near you. Here's a look at the most common internet scams—and what you can do to safeguard your personal information and wallet.

COVID-19 Online Scams

According to Google, "Scammers are taking advantage of the increase in COVID-19 communications by disguising their scams as legitimate messages about the virus. Alongside emails, scammers may also use text messages, automated calls and malicious websites to reach you."

Common types of COVID-19 scams include:

- Fake health organizations. Scammers pose as health authorities like the World Health Organization (WHO) and U.S. Centers for Disease Control (CDC) to offer cures, tests, or other COVID-19 information.
- Websites that sell fake products. These sites offer face masks, hand sanitizer, disinfectant wipes, and other high-demand products that never arrive. Buy products from known marketers only.
- Bogus government sources. These scammers claim to issue updates and payments on behalf of the Internal Revenue Service (IRS) or local tax authority.
- Fraudulent financial offers. Scammers may pose as banks, debt collectors, or investors with offers designed to steal your financial information.
- Fake nonprofit donation requests. Many people like to donate to charitable causes to help with disaster relief. This provides an excellent opportunity for scammers to set up fake nonprofits, hospitals, and other organizations to collect funds. Donate directly through a reputable nonprofit's website instead of clicking on a link you receive by email or text.

Disaster Relief Scams

When disaster strikes—whether it's a pandemic or weather-related—so do fraudsters. Hiding behind the guise of an actual aid organization, scammers will use a tragedy or natural disaster to con you out of your money. By thinking you are donating to an emergency relief fund, you unwittingly provide credit card or other e-payment information. Only give to established, legitimate organizations. Always verify the validity of any charitable organization you are considering supporting before you donate.

Phishing Scams

You receive an email from a seemingly familiar enterprise that you deem legitimate, such as your bank, university or a retailer you frequent. The message directs you to a site—usually to verify personal information such as email addresses and passwords—that then steals your information and exposes your computer to attack by scammers. Phishing scams are some of the most common attacks on consumers. According to the FBI, more than 114,700 people fell victim to phishing scams in 2019. Collectively, they lost $57.8 million, or about $500 each. According to the Federal Trade Commission, phishing emails and text messages frequently tell stories to trick people into clicking on a link or opening an attachment.

For example, phishing attempts may:

- Say they've noticed suspicious activity or log-in attempts on your account
- Claim there's a problem with your account or payment information
- Say you need to confirm or update personal information
- Include a fake invoice
- Ask you to click on a link to make a payment
- Claim you're eligible to sign up for a government refund
- Offer a coupon for free goods or services

You should never click the links provided in emails you can't independently confirm. Doing so will make your computer and personal information vulnerable to viruses and malware. Again, though the sender may seem legitimate—which is exactly what the scammer wants you to believe—no reputable institution will ask for your password or other key personal information online. Phishing emails will often contain typos or grammatical errors, and the sender's email address often looks suspicious.

In remembrance of George William Barnes (1954-2020)

Fake Shopping Websites & Formjacking

Thousands of fake websites offer "great deals" on well-known brands. These websites typically have URLs similar to the brands they try to mimic, such as Amazon.net. If you buy something from one of these websites, chances are you'll receive a counterfeit item in the mail—or nothing at all.

Formjacking is another retail scam. This happens when a legitimate retail website is hacked, and shoppers get redirected to a fraudulent payment page, where the scammer steals your personal and credit card information. To avoid this scam, double-check that the URL on the payment page is the same as the website where you were shopping. Cybercriminals may change the URL very slightly—maybe by adding or omitting a single letter. Be sure to take a close look at the URL before you enter your payment details.

Tech Support Scams

With this scam, you receive a phone call, email, or pop-up warning indicating your computer is infected (ask yourself: How would they know?). The scammer then:

- Prompts you to download an application that allows them to control your computer remotely;
- Downloads an actual virus or otherwise makes you believe that something is wrong; and
- Tells you they can fix the problem for a fee.

Another way to reach you is through search results: Tech support scammers work hard to get their websites to show up in online search results, or they run their own ads.

Often, these scammers ask you to pay using a bank wire, gift card, or money transfer app.

If you gave a scammer remote access to your computer, immediately update your security software, run a thorough scan, and delete anything it identifies as a problem. And, if you shared your username and password, change those right away, too.

Fake Antivirus Software (aka "Scareware")

Fake antivirus software ads and pop-ups try to make you believe your computer is infected with a virus (or dozens of them)—and that you can fix the problem by downloading their software. These scammers get you two ways:

1. They gain access to your credit card information.
2. They gain access to your computer. When you click the download link, you get a virus, malware, or ransomware instead of antivirus software. According to Norton, "The scammers can use this malware to access your files, send out fake emails in your name, or track your online activity."

Always be wary of ads and pop-ups that prompt you to take immediate action, or ones that are hard to close. Be sure to install, update, and use real antivirus software to reduce the risk of scareware.

Travel Scams

New for 2020 and beyond are scammers that sell phony COVID-19 travel insurance policies that claim to cover losses for any reason, at no extra charge. Buyers find out the hard way that these policies do not provide the protection they expected. In general, claims due to "known, foreseeable, or expected events, epidemics, government prohibitions, warnings, or travel advisories or fear of travel" are not covered by travel insurance policies.

COVID-19 is a foreseen event, so many travel insurance coverages don't apply. The only way to get coverage for COVID-19-related losses is to buy a Cancel for Any Reason (CFAR) policy directly from a licensed, reputable company. These policies usually cost significantly more than standard travel insurance policies.

Another travel scam involves social media. Scammers post enticing photos on sites like Pinterest, Twitter, and Instagram to dupe even the savviest of travelers. Upon clicking the image—which lures clicks through the promise of a free trip or plane tickets—you will be prompted to either complete a survey rife with personal information or open your computer up to secretly malicious software.

Make sure the social media page you're on is an accredited account. All major airlines and travel sites link directly to their social media handles from their respective web pages.

Grandparent Scams

With grandparent scams, a fraudster poses as a panicked grandchild who needs cash right away for some emergency—to get out of jail, leave a foreign country, or pay a hospital bill. The COVID-19 pandemic has made it even easier to sell compelling lies: "Grandma, I'm in the hospital with COVID. Please send money right away." AARP says that grandparent scams are on the rise, with nearly $41 million in reported losses during 2018, up from $26 million the year before.

In remembrance of George William Barnes (1954-2020)

According to the FTC, you can avoid grandparent scams (and other family emergency scams) if you:

- Resist the urge to act immediately. Scammers pull at your heartstrings and rely on you to respond quickly—before you've had a chance to think things through.
- Verify the caller's identity. Ask questions that a stranger would not be able to answer. Confirm the story with other family members or friends, even if (or especially if) the caller says to keep it a secret.
- Never send cash, gift cards, or money transfers.

419 Fraud – Advance Fee Scam

Also known as the Nigerian letter scam, 419 fraud is one of the most common scams on the internet—and one you've likely seen in your own inbox. The advance fee scheme takes its name after the section of the Nigerian criminal code that outlaws fraud. According to the FBI, more than 14,600 people reported falling victim to advance fee scams in 2019. Collectively, they lost $100.6 million, or roughly $6,800 each.

The scammer usually claims to be a member of a wealthy Nigerian or another West African family, reaching out to you personally after the death of a loved one. He or she seeks to relocate a large fortune out of the country for safekeeping purposes and into your bank account. The catch? You must submit small payments for fees in return for a large chunk of their cash cache.

You should never respond to these requests or volunteer your bank details.

Pre-Approved Notice

You receive a letter or an email declaring that you have been pre-approved for either a credit card or a bank loan. Those experiencing financial strain may fall victim to this scam, which promises instant approval and appealing credit limits. The catch? You must pay an upfront fee when you sign up. While credit card companies do charge annual fees, they will never ask you to pay them when you apply.

In general, be wary of any offer that has a "100% guarantee," requires any upfront fees, or that requests payments in cash, money transfers, or gift cards.

Debt-Relief and Credit-Repair Scams

Individuals who are down on their luck can easily fall for an email claiming to relieve their debt or repair bad credit. This scam makes the false promise to negotiate with creditors to either consolidate or settle debts, or to remove negative information from your credit report.

According to the Federal Trade Commission (FTC), "These operations often charge cash-strapped consumers a large up-front fee, but then fail to help them settle or lower their debts—if they provide any service at all."

Steer clear of any debt-relief company that asks for fees in advance, before it settles any debt. Likewise, avoid any company that guarantees it can eliminate or reduce your debt by X amount by X date. Research any debt-relief or credit-repair service you are considering. It's a good idea to check with your state's attorney general and consumer protection agency to learn about the company's reputation.

Lottery Scam

Congratulations! You've won the lottery or some other large amount of money! Except you haven't. This bogus email comes to you out-of-the-blue—usually claiming to be a part of international sweepstakes—stressing you've won big and that you just need to send over a processing fee or get in touch with someone who can process your winnings.

Unless you have entered some legitimate lottery, chances are you haven't won the jackpot. When you win the lottery, you contact the appropriate retailer—not the other way around.

Fake Check or Money Transfer

You list something on an auction-based website, and the winning bidder offers to pay you more than the offered purchase price via cashier's, corporate or personal check. Upon receiving the scammer's counterfeit check, you are conned into sending the difference back through bank wire. Then you have to pay the bank back in full once the fake check bounces.

Never accept payment for more than your selling price. Additionally, you should opt for a secure form of e-payment, such as PayPal or Google Wallet, to ward off scammers.

In remembrance of George William Barnes (1954-2020)

INVESTIGATOR OF THE MONTH:

Chris Porter – Kavod Polygraph Services

Why use Polygraphs?

Lie Detection and the Polygraph:

For as long as human beings have deceived each other, people have tried to develop techniques for detecting deception and determining the truth (see e.g., Kleinmuntz and Szuko, 1984). These tchniques have almost always included interviews and interrogations to try to see through deception and reveal what a deceiver will not freely admit. In the 20th century, lie detection took on specific aspects with the development of techniques that use measures of psychological responses as indicators of deception. The most reliable of these is the polygraph. This technique, which relies on physiological measurements, has become for many in the intelligence communities (including counterintelligence officials in Government agencies) the most valied method for identifying criminals, spies, and saboteurs when direct evidence is lacking.

Polygraph examinations are widely used in the South Africa and in some other countries (notably, America, Europe, Israel, Japan and Canada) for these purposes:

Specific Issue Polygraph Testing (Theft, fraud, assault, etc.)

Criminal investigation is one of the major fields in which polygraph tests are employed to detect lying.

Polygraph tests are useful not only to identify the criminals who might try to deceive the legal systems, but it will also be helpful for providing justice to several innocent victims.

Anothr important inductrial application of polygraph tests according to Walczyk et. Al. (2005) is to discover employee thefts.

Employee theft is a growing concern for organizations as it tends to cause the firms huge burden.

Labour Related Polygraph Testing (Pre-employment, pre-promotion, annual screening / periodic)

Industrial or business application is an important use of polygraph tests. They can contribute significantly in enhancing organizational effectiveness.

Selecting candidates with the right skills and experience as well as promoting employee honesty in the workplace are important aspects of effective and successful organizations However, in recruitment, the job applicants may not be truthful on their job applications. They migh dishonestly claim possessing the relevant skills and experience in order to qualify for employment (Walczyk, Schwartz, Clifton, Adams & et. Al. 2005).

Walczyk, et. al. (2005) noted that if firms failed to identify such falsified or dishonet applicants, it might cost them significantly. Dishonest job applicants are extremely expensive to organizations as it might lead to considerable waste of investent such as time and money for recruitment.

Infidelity

Suspect your partner may be unfaithful?

With the proper evidence, ou can finally move boyond the lies. Betrayal from a loved one is one of the most distressful things to go through in life. It can be difficult to seek out assistance in these life changing circumstances.

With polygraph proof of the infidelity, you can finally move past the lies and choose to repair your relationship or move on.

In remembrance of George William Barnes (1954-2020)

kavod

POLYGRAPH SERVICES

KAVOD POLYGRAPH SERVICES PTY LTD

Registration number: 2019 / 111762 / 07

TAX Number: 9004694270

B-BBEE: Level Four

www.kavodpolygraphservices.co.za kavodps@gmail.com 082 418 6616

SOME TESTING GUIDELINES

Before meeting with the examinee, the polygraph examiner and the investigator, or client, will discuss the merits of the case to give the examiner some background. The examiner, together with the investigator, or client, will then formulate the 'Relevant Questions', which are the target test questions.

The target test questions, or 'Relevant Questions', have to conform to very strict regulations and to the science behind the psychology of the polygraph.

Polygraph examinations take approximately one to one and a half hour per test. The room in which the test will be conducted must be clear of noise (audible and visible). The examinee must be well rested and in good health.

It is important to note that a polygraph examination can only be conducted after signed consent is received from the examinee. The examinee has the right to refuse testing.

The examination consists of four parts; it first starts with an introduction during which the rights of the examinee are explained and consent is obtained; that follows with a pre-test interview with the examinee in order to build the psychological set in the mind of the person that is about to be tested; following that, the in-test phase will commence in which test data will be recorded when presented with the stimuli in the form of several test questions using the Lafayette Computerized Polygraph System. Data will be analyzed and scored during this phase. After this, the post-test phase will commence in which the examiner may ask the examinee any clarifying questions.

Results will be made available within 24 hours of testing.

We use the latest in techniques and our equipment are regularly checked for accuracy.

In remembrance of George William Barnes (1954-2020)

SERVICES INCLUDE THE FOLLOWING

- **Specific Issue Polygraph Testing** *(Theft, fraud, assault, etc.)*

  Criminal investigation is one of the major fields in which polygraph tests are employed to detect lying.

  Polygraph tests are useful not only to identify the criminals who might try to deceive the legal systems, but it will also be helpful for providing justice to several innocent victims.

  Another important industrial application of polygraph tests according to Walczyk et.al. (2005) is to discover employee thefts.

  Employee theft is a growing concern for organizations as it tends to cause the firms huge burden.

- **Labour Related Polygraph Testing** *(Pre-employment, pre-promotion, annual screening / periodic)*

  Industrial or business application is an important use of polygraph tests. They can contribute significantly in enhancing organizational effectiveness.

  Selecting candidates with the right skills and experience as well as promoting employee honesty in the workplace are important aspects of effective and successful organizations. However, in recruitment, the job applicants may not be truthful on their job applications. They might dishonestly claim possessing the relevant skills and experience in order to qualify for employment (Walczyk, Schwartz, Clifton, Adams & et.al. 2005).

  Walczyk, et.al. (2005) noted that if firms failed to identify such falsified or dishonest applicants, it might cost them significantly. Dishonest job applications are extremely expensive to organizations as it might lead to considerable waste of investment such as time and money for recruitment.

- **Infidelity Testing**
- **Testifying as an expert witness at Disciplinary Hearings, Labour Courts (CCMA) & Criminal Courts**
- **Arrests**

OTHER SERVICES INCLUDE

- **Criminal Record Check**

  Employers have become increasingly aware of the importance of knowing if an applicant has a criminal record. Employers have a legal duty to make reasonable inquiries about who they hire, and to provide a safe workplace. An employer who hires a person with a criminal record can be found liable for negligent hiring where the hiring decision results in harm, and it could have been avoided by a simple criminal record check. Checking criminal records demonstrates Due Diligence and is also an important preventative measure to protect against workplace violence.

- **ITC Credit Check** *(Credit Bureau)*

  The National Credit Act (NCA) makes provision for employers to check a candidate's credit status when they are applying for a job that requires trust and honesty.

  Assessing a candidate's financial situation enables the employer to determine aspects of that person's character, their personal context at the time of screening, and how that character and context will influence their performance at work. An irregular credit report can highlight a person's overall lack of responsibility, such as missed payments, a bankruptcy, or multiple judgements.

Polygraph examinations can be conducted anywhere in Southern Africa
(including Lesotho, Mozambique, Zimbabwe, Botswana and Namibia).

Alternatively, examinees can be brought to our offices in Fourways where we regularly conduct polygraph examinations in a quiet and security controlled area.

CONTACT US FOR AN OBLIGATION-FREE QUOTE.

In remembrance of George William Barnes
(1954-2020)

FERLIO NOTIFICATION BOARD

JANUARY BIRTHDAYS

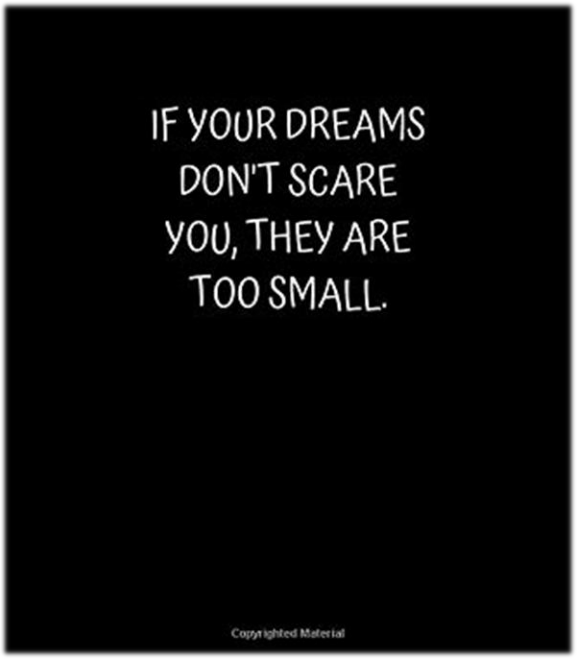
We here at Ferlio wish you have a wonderful birthday and a prosperous year ahead.

- Peet Labuschagne – 03 January
- Dave De Wet – 07 January
- Ricardo Gasper – 09 January
- Riaan Mulder – 12 January
- Pierre Loock – 17 January
- Eric Goosen – 18 January
- Gert Van Staaden – 19 January
- Johan (Bossie) Boshoff – 21 January
- Derrick Bothma – 23 January
- Tania Spinnler – 31 January
- Drienie Vorster – 01 February

HAPPY NEW YEAR

We at Ferlio would like to wish all readers a prosperous new year 2021.

MOTIVATION FOR THE MONTH:



In remembrance of George William Barnes (1954-2020)

Ferlio

Group of Investigators

SPECIALIST SERVICES OFFERED:

Investigations, including but not limited to:
- Criminal
- Civil
- Forensic
- Cyber

Profiling
- Profiling / Lifestyle audit of individuals
- Business profiling
- Strategic audits on business
- Fingerprint screening
- Financial Audit Investigations
- Employee Background Screening
  - Identification documents
  - Driver's License & PDP
  - Criminal record
  - Educational background & qualifications
  - Prior employment records
  - Credit status
  - Integrity testing
  - Identification photos
  - Fingerprint verification

Undercover agents
- Standard level agents
- High level agents
  - Strategic level agents

Surveillance
- Physical
- Static
- Electronic
- Counter
- Covert escorting

Close Protection
- Executive protection
- Executive Support
- Asset in transit protection

Handwriting Specialist & Fingerprint Specialist

Polygraphs

Fraud Detection Initiatives

Security Risk Assessments

Transcripts / Translations

Pre-employment Psychometric Assessments

Truck & Driver Inspections

Security Vulnerability Assessment

GET IN TOUCH:

Phone: 0860 337 546 / 0860 (F-E-R-L-I-O)

Email: office@ferlio.co.za

Find us on Facebook: @FerlioGroupOfInvestigators

Ferlio Group of Investigators
@FerlioGroupOfInvestigators · Private Investigator

In remembrance of George William Barnes (1954-2020)