



# Women & cybersecurity:

Investigating cybercrimes against women in the continent of Africa stemming from gender inequalities, and identifying strategies to combat this phenomenon.

JULY 2023

# ABSTRACT

Cybercrime is defined as a type of crime involving a computer or a computer network. The annual cost of global cybercrime is now estimated to be \$600 billion, up more than \$100 billion from four years ago (Mountrouidou, X., Vosen, D., Kari, C., Azhar, M. Q., Bhatia, S., Gagne, G., Maguire, J., Tudor, L., & Yuen, T. T., 2019). In terms of cybercrime, globalization translates into perpetrators and victims in far-flung regions, diminishing both the possibility and the incentive for law enforcement action (Mountrouidou, X., Vosen, D., Kari, C., Azhar, M. Q., Bhatia, S., Gagne, G., Maguire, J., Tudor, L., & Yuen, T. T., 2019). This paper will discuss the issue of cyber crime within the continent of Africa and the implication of the preceding gender inequality towards women regarding this matter. Solutions to this issue will also be presented.

## Author

Ndeye Aminata Thiome  
GTI-U Intern 2023



# Introduction

While the number of cybersecurity attacks worldwide have grown substantially, the 2017 International Telecommunications Union Cybersecurity Index reported a lagging national response, with only 38% of member countries having a cybersecurity strategy with the lowest commitment level in Sub-Saharan Africa (Wechsler, M., & Siwakoti, S., 2022). An African cybersecurity firm estimated that cybercrime costs the region USD 3.5 billion annually and a survey suggested that a substantial majority of African businesses operate well below acceptable cybersecurity practices (Wechsler, M., & Siwakoti, S., 2022). A 2018 survey of six African countries by the Global Cybersecurity Capacity Centre (GCSCC) noted that all lacked a national cybersecurity awareness program and described efforts as being in an embryonic stage with “extremely low ICT literacy levels which hinder any design of cybersecurity campaigns and that executive members in organizations myopically underestimate the problem (Wechsler, M., & Siwakoti, S., 2022).” It would appear that greater priority should be placed in the cybersecurity sector for developing countries, especially as the new era of smartphones advances and will create further challenges for consumers who may possess notably lower levels of technical literacy and cybersecurity awareness (Wechsler, M., & Siwakoti, S., 2022).

In a research study conducted by researchers, Michael M. Wechsler and Samikshya Siwakoti that focused in on developing countries in Africa and South Asia, it was found that women may be more susceptible than men to malfeasances and other concerns related to cyber risks and cyber fraud as a result of inequalities and gender gaps that exist within developing countries (Wechsler, M., & Siwakoti, S., 2022). Women consistently ranked behind men with regard to access to, use of and experience with information and communication technologies, ownership of mobile hardware and Digital Financial Services (DFS) (Wechsler, M., & Siwakoti, S., 2022). Women were also perceived to possess lower digital and language literacy rates and subjected to limiting social, cultural, religious and legal barriers (Wechsler, M., & Siwakoti, S., 2022). These factors often tied them to roles in private spaces, such as the family home; as such, access to important peer knowledge networks which disseminate timely information about cybersecurity and fraud issues was limited, which often occur in public spaces (such as the workplace, in the marketplace and social settings) (Wechsler, M., & Siwakoti, S., 2022). As a result, women’s overall cyber awareness and cyber hygiene levels would likely be lower than men, including their capabilities to combat social engineering related fraud which appears to present a formidable challenge in developing countries (Wechsler, M., & Siwakoti, S., 2022).

All of the aforementioned topics will be discussed; first beginning with the societal/household dynamics within African developing countries, then access to education will be discussed. This will be followed by discussions on access to technology within developing countries in Africa and the Cybersecurity threats that are faced by women. To conclude, recommendations regarding these cybercrimes against women will be discussed.

# TABLE OF CONTENTS

Abstract

Introduction

Societal/Household Dynamics 1-2

Access To Education 3-4

Access To Technology 5-6

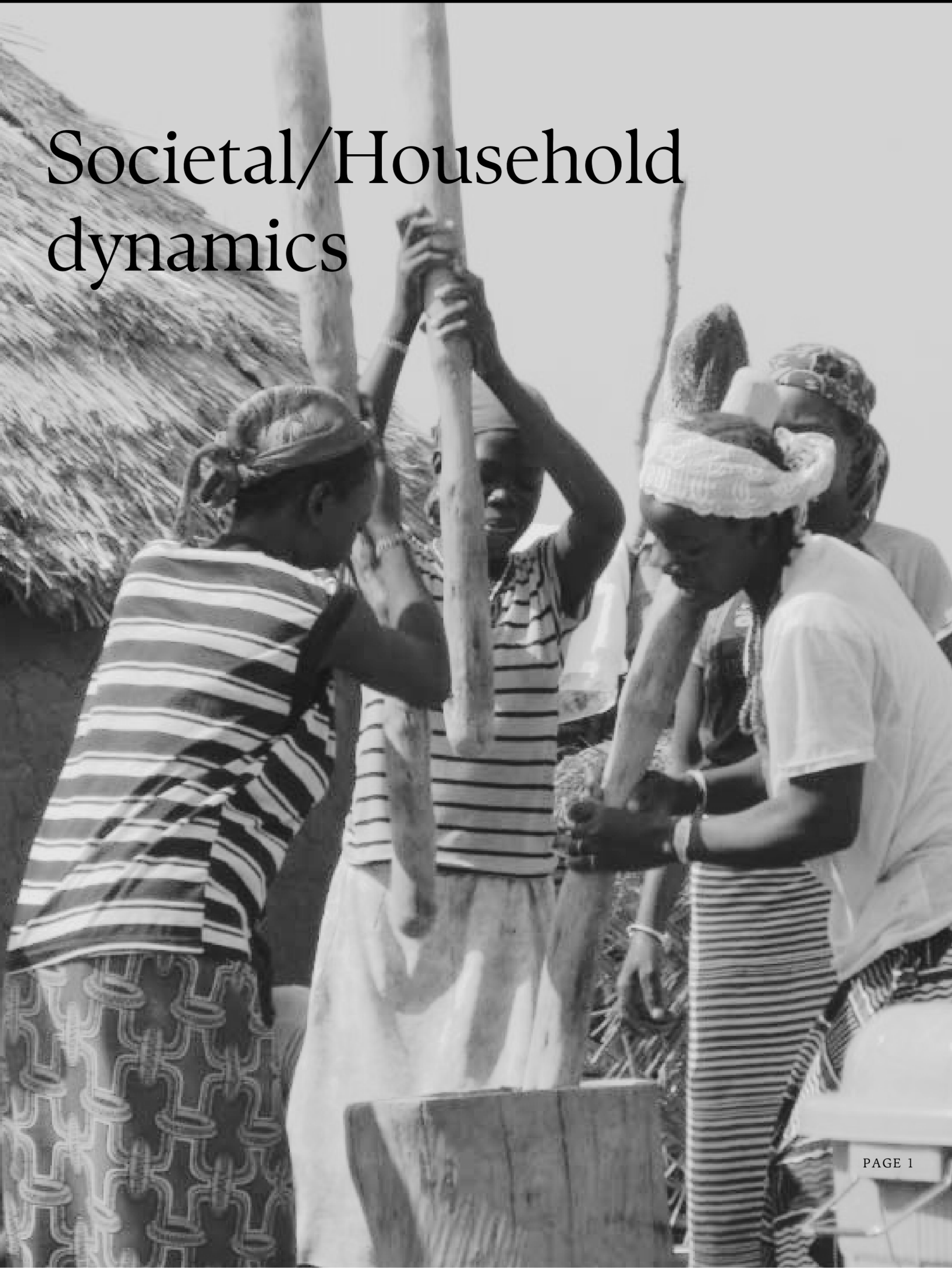
Cybersecurity Threats 7

- Digital Financial Services 8-10
- Sexual Harassment 11
- Smishing 12-13
- Phishing 14-15
- Vishing 16
- Pretexting/Impersonation 17-18
- Frauds 19-20

Recommendations 21-23

References 24

# Societal/Household dynamics





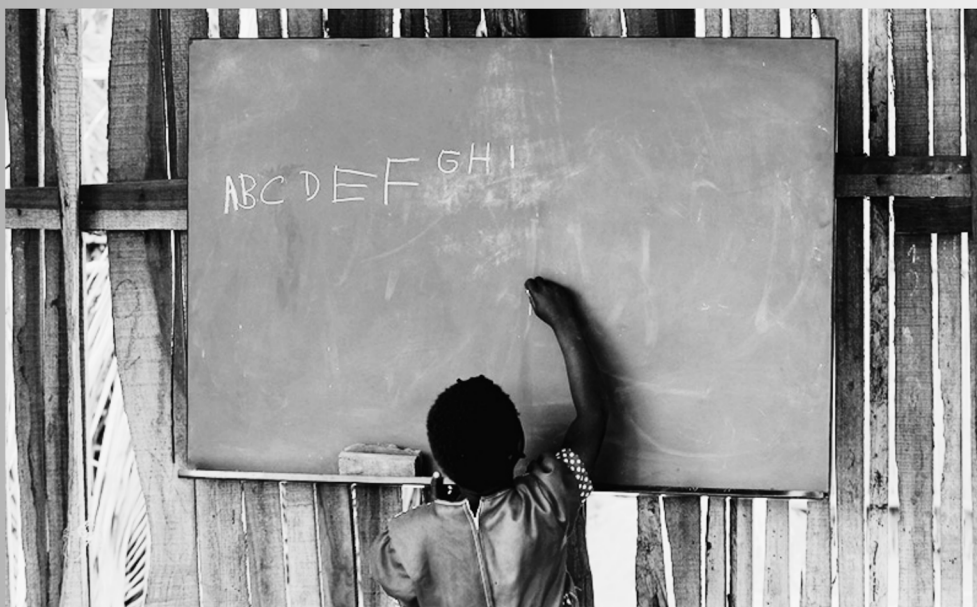
Some conservative and religious environments with patriarchal gender norms can emphasize the role of women primarily as child bearers and household custodians rather than breadwinners, which can place less emphasis on their access to education and reduce their social mobility (Wechsler, M., & Siwakoti, S., 2022). Along with this, in developing countries males are often head of household, thus in charge of finances and first in priority for ICT access (Wechsler, M., & Siwakoti, S., 2022). Women have notably lower language literacy levels, economic opportunities and DFS account ownership levels than men, in addition to unique onboarding hurdles in some jurisdictions (Wechsler, M., & Siwakoti, S., 2022). Among those without a financial bank account, 14 countries had double digit gender gaps led by Morocco (15%), Bangladesh (15%) and Algeria (13%) (Wechsler, M., & Siwakoti, S., 2022). In Africa, Nigeria and Mozambique had substantial double-digit gender gaps in both categories (Wechsler, M., & Siwakoti, S., 2022). Only 43% of adults had a financial account and 58% of women owned a mobile phone compared to 71% of men (Wechsler, M., & Siwakoti, S., 2022). These barriers can reduce incentive in women to build DFS- related knowledge, capacity and comfort with technology which potentially reduces awareness of and increases vulnerability to cybersecurity risks and fraud (Wechsler, M., & Siwakoti, S., 2022).

While possession of a verified identity is relatively high among unbanked adults, the Global Findex data indicates an average of 8% fewer women own a national identity card across Sub-Saharan Africa, with sizable double-digit gender gaps in Afghanistan (46%), Pakistan (14%), Ethiopia (20%) and Mozambique (14%) (Wechsler, M., & Siwakoti, S., 2022). The World Bank's ID4D-Findex study reported that the difference in ID ownership between men and women exceeds 20 percentage points in Chad, Niger, Benin and South Sudan (Wechsler, M., & Siwakoti, S., 2022). Legal and regulatory hurdles in Cameroon, Chad, Gabon, and Niger make the process of opening a bank account more challenging specifically for women, as is the case in other areas such as Bangladesh due to substantial social and cultural gaps (Wechsler, M., & Siwakoti, S., 2022).

Lower DFS account ownership numbers among women can stem from several factors in developing countries, especially those with strong conservative, religious and patriarchal influences, such as: traditional gender roles where males are expected to have greater financial literacy and are in control of household finances; lower women's literacy and numeracy levels which makes use of DFS challenging; and the propensity to default to over-the-counter (OTC) transactions if readily available – where transactions are conveniently offloaded to agents using their own accounts to conduct transfers on behalf of women without DFS accounts (Wechsler, M., & Siwakoti, S., 2022).

# Education Access

Moving towards adulthood, a United Nations (UN) study of women's levels of educational participation revealed that women in Sub-Saharan Africa and SA were well below gender parity levels for primary educational levels, with a substantial drop in upper secondary education (Wechsler, M., & Siwakoti, S., 2022). Women tend to marry at comparatively younger ages in countries in Sub-Saharan Africa, Middle East and North Africa and South Asia and may drop out of school to take care of family (Wechsler, M., & Siwakoti, S., 2022). This leads to low literacy and numeracy rates for women, leading them to having a high reliance on orality, which creates additional challenges to use and understand technology and financial transactions (Wechsler, M., & Siwakoti, S., 2022). In Kenya where the national literacy rate is high at 79%, mean years of schooling are only 5.7 years for girls versus 7.1 years for boys (Wechsler, M., & Siwakoti, S., 2022). Traditionally, women in Kenya have been steered away from study and occupations involving science, technology, engineering and math (STEM) and towards social sciences and "women's jobs" such as general marketplace opportunities and agriculture (Wechsler, M., & Siwakoti, S., 2022). While initiatives have been in place to increase participation in STEM studies and cybersecurity opportunities, cultural and social barriers still impact on young women, including challenges to be accepted into and study at secondary education levels which focus on cybersecurity and STEM subjects (Wechsler, M., & Siwakoti, S., 2022).



GSMA surveys (appearing in Exhibit 7) found that low language and technical literacy skills were among the top barriers to owning a mobile phone by non-phone owners, with low awareness of an understanding of the Internet in Africa and Asia (Wechsler, M., & Siwakoti, S., 2022). Also observed was that women possess lower mobile technical literacy levels than men since they also trail with (i) lower levels of mobile phone ownership; (ii) lower literacy and educational levels (reading and writing, especially in Sub-Saharan Africa); and (iii) lower confidence levels in their ability to operate the phone. It was also found that (Wechsler, M., & Siwakoti, S., 2022):

- Women in the bottom of the pyramid in rural areas may generally lack awareness and knowledge about basic DFS product and service information, pricing, and resolution mechanisms;
- Cyber awareness and technical capacity of women is likely low at the time of onboarding; customer education may be limited at the agent level as focus is often primarily on sales with basic attention to security training; family members may supplement cyber awareness to a moderate degree;
- While MNOs, DFSPs and governmental authorities related to ICT may attempt to push information to the masses with regard to cyber awareness and hygiene, it is often limited in effectiveness and very low on the grassroots level.
- Cyber awareness and technical capacity of women may remain lower than men after onboarding as women's peer knowledge networks – a critical component of post-onboarding support – are typically not as robust, informative and substantive as men's networks;
- Adult women's lower literacy and numeracy levels impact on their basic understanding of the financial and technical parts of DFS and may be further compounded when English is used for DFS and is not provided in the customer's native language;
- Automatic and Unread SMS Transmissions – such as ignoring text messages – is an increasingly common practice among women with low literacy levels which can make important and timely security warnings and alerts ineffective.

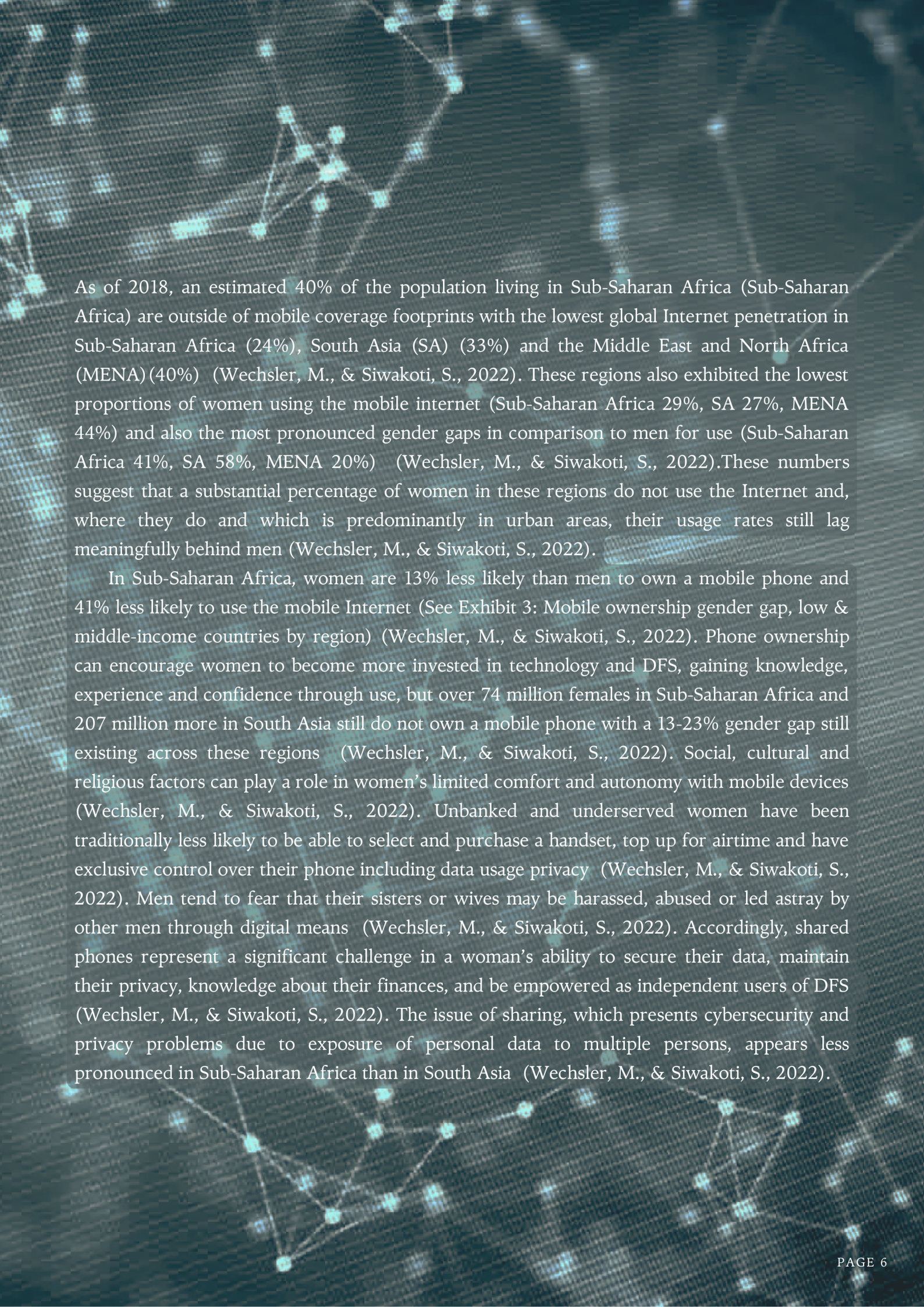
	Don't know how to use a phone		Reading/Writing difficulties		Strangers contacting me		Family does not approve	
Country	Men	Women	Men	Women	Men	Women	Men	Women
Algeria	22%	27%	21%	30%	5%	5%	3%	21%
Kenya	0%	7%	15%	26%	6%	5%	0%	3%
Mozambique	6%	24%	16%	28%	2%	6%	2%	9%
Nigeria	9%	16%	45%	49%	4%	6%	6%	22%
Senegal	7%	7%	28%	30%	6%	18%	6%	4%
South Africa	3%	10%	10%	16%	0%	12%	3%	6%
Uganda	12%	15%	23%	21%	3%	4%	4%	10%
Bangladesh	19%	31%	46%	21%	0%	1%	6%	11%
India	11%	16%	18%	24%	12%	7%	3%	9%
Indonesia	21%	27%	36%	32%	4%	11%	1%	7%
Myanmar	40%	43%	22%	20%	13%	12%	2%	9%
Pakistan	10%	13%	56%	38%	5%	13%	7%	38%

#### Exhibit 7: Important barriers to owning a mobile phone

Percentage of non-mobile owners who identified the following as the single most important barrier to owning a mobile. 2019 Base: Non-mobile owners aged 18+ Mobile ownership is defined as a person having sole or main use of a SIM card (or a mobile phone that does not require a SIM), and using it at least once a month. See footnote for details. *Source: GSMA Intelligence Consumer Survey, 2019.*<sup>95</sup>

# Access To Technology





As of 2018, an estimated 40% of the population living in Sub-Saharan Africa (Sub-Saharan Africa) are outside of mobile coverage footprints with the lowest global Internet penetration in Sub-Saharan Africa (24%), South Asia (SA) (33%) and the Middle East and North Africa (MENA) (40%) (Wechsler, M., & Siwakoti, S., 2022). These regions also exhibited the lowest proportions of women using the mobile internet (Sub-Saharan Africa 29%, SA 27%, MENA 44%) and also the most pronounced gender gaps in comparison to men for use (Sub-Saharan Africa 41%, SA 58%, MENA 20%) (Wechsler, M., & Siwakoti, S., 2022). These numbers suggest that a substantial percentage of women in these regions do not use the Internet and, where they do and which is predominantly in urban areas, their usage rates still lag meaningfully behind men (Wechsler, M., & Siwakoti, S., 2022).

In Sub-Saharan Africa, women are 13% less likely than men to own a mobile phone and 41% less likely to use the mobile Internet (See Exhibit 3: Mobile ownership gender gap, low & middle-income countries by region) (Wechsler, M., & Siwakoti, S., 2022). Phone ownership can encourage women to become more invested in technology and DFS, gaining knowledge, experience and confidence through use, but over 74 million females in Sub-Saharan Africa and 207 million more in South Asia still do not own a mobile phone with a 13-23% gender gap still existing across these regions (Wechsler, M., & Siwakoti, S., 2022). Social, cultural and religious factors can play a role in women's limited comfort and autonomy with mobile devices (Wechsler, M., & Siwakoti, S., 2022). Unbanked and underserved women have been traditionally less likely to be able to select and purchase a handset, top up for airtime and have exclusive control over their phone including data usage privacy (Wechsler, M., & Siwakoti, S., 2022). Men tend to fear that their sisters or wives may be harassed, abused or led astray by other men through digital means (Wechsler, M., & Siwakoti, S., 2022). Accordingly, shared phones represent a significant challenge in a woman's ability to secure their data, maintain their privacy, knowledge about their finances, and be empowered as independent users of DFS (Wechsler, M., & Siwakoti, S., 2022). The issue of sharing, which presents cybersecurity and privacy problems due to exposure of personal data to multiple persons, appears less pronounced in Sub-Saharan Africa than in South Asia (Wechsler, M., & Siwakoti, S., 2022).

# Cybersecurity Threats

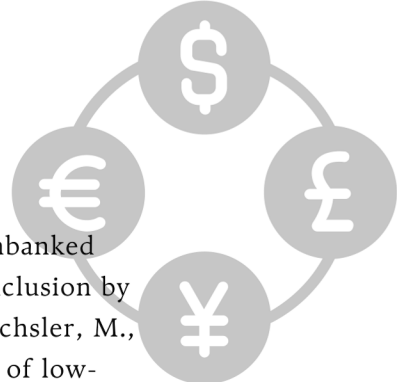


Cybersecurity and fraud issues relating to DFS in which a gender influence may be perceived are those issues which concern or target humans and their behavior rather than machines (Wechsler, M., & Siwakoti, S., 2022). The predominant issues are social engineering frauds, identity theft, monetary scams, cybersecurity awareness and hygiene (Wechsler, M., & Siwakoti, S., 2022). The issue of how gender may play a role in customer cybersecurity practices and susceptibility to DFS fraud is a complex issue (Wechsler, M., & Siwakoti, S., 2022). It can be the product of many factors and influences – social, cultural, biological, and psychological, among others (Wechsler, M., & Siwakoti, S., 2022). As opposed to cybersecurity attacks targeting digital devices, social engineering attacks and DFS scams target humans and their behavior patterns, which can be influenced by factors such as gender (Wechsler, M., & Siwakoti, S., 2022). Attacking human weakness is the predominant method of cybersecurity attacks in DFS (Wechsler, M., & Siwakoti, S., 2022).

The increase of social engineering attacks, especially in developing countries, may be rooted in its relatively low barriers to entry, efficiency and scalability (Wechsler, M., & Siwakoti, S., 2022). It relies less on the technological skills (and gender) of the attacker and more on exploiting basic human psychology – anticipating how a population tends to react to specific situations (Wechsler, M., & Siwakoti, S., 2022). Attacks may be optimized, tailored and refined over time for a target population, such as a poorer, less educated group of persons in a developing country who may predominantly use basic and feature phones (Wechsler, M., & Siwakoti, S., 2022). Women in developing countries can experience notably higher levels of inequality compared to men and may experience varying degrees of marginalization and discrimination resulting in more limited opportunities for capacity building and economic and social mobility (Wechsler, M., & Siwakoti, S., 2022). This can profoundly affect women's exposure to ICT and DFS, the manner in which they approach, understand and use technology and DFS, and their general levels of awareness of that which may be impacting within the realm of cybersecurity and digital fraud issues they may encounter (Wechsler, M., & Siwakoti, S., 2022). Regional consultants, central banks and MNOs we consulted repeatedly emphasized social engineering as a predominant problem confronting DFS users and providers due to low levels of digital literacy, cyber awareness and cyber hygiene present locally and the simplicity and effectiveness of the attacks (Wechsler, M., & Siwakoti, S., 2022).

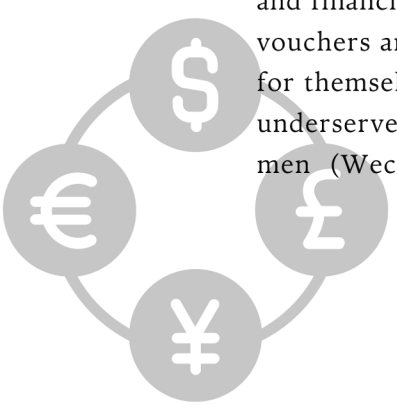


# Digital Financial Services



Digital Financial Services is intended to address the needs of the poor, unbanked and underserved in developing countries, aspiring to improve financial inclusion by shifting the provision of financial services from banks to non-banks (Wechsler, M., & Siwakoti, S., 2022). Access is provided predominantly through the use of low-cost mobile phones providing basic functionality which acts as a payment instrument utilizing a mobile money transfer system where mobile wallets are linked to telephone numbers (Wechsler, M., & Siwakoti, S., 2022). The DFS bouquet of products and services includes payments and remittances, savings, loans, investments, insurance among others (Wechsler, M., & Siwakoti, S., 2022). Many of these services are offered by Mobile Network Operators (MNOs) and Digital Financial Service Providers (DFSPs) (Wechsler, M., & Siwakoti, S., 2022). A majority of the poorest members of the population reside predominantly in rural areas, regions which feature limited mobile coverage and power availability (Wechsler, M., & Siwakoti, S., 2022). Mobile infrastructure still makes it possible to overcome operational barriers in these areas and make financial services increasingly accessible and affordable to residents (Wechsler, M., & Siwakoti, S., 2022). Most frontline services, such as customer signup and cash-related services such as Cash-in and Cash-out (CICO) operations are performed by commissioned DFS ‘agents’ contracted to DFS providers who are situated in strategic locations across rural areas (Wechsler, M., & Siwakoti, S., 2022). As aforementioned, social engineering is an attack on humans – rather than machines – who control access and authorization to electronic data, information and computer networks (Wechsler, M., & Siwakoti, S., 2022). It is the art of manipulating people into performing a desired action under false pretenses, often for the purpose of reaping financial reward (Wechsler, M., & Siwakoti, S., 2022). Social engineering presents a cyberattack that frequently affects DFS (Wechsler, M., & Siwakoti, S., 2022). It relates to human behavior which can be influenced by gender factors, which are examined in this section (Wechsler, M., & Siwakoti, S., 2022).

Taken as a whole, women at the bottom of the pyramid– especially in rural areas – appear to be consistently lagging behind men regarding the technology they use, their access to and use of DFS in being: notably less likely to own a mobile phone; less likely to own a smartphone; less likely to have or make use of Internet access; more likely to face literacy and numeracy challenges; less educated overall with less financial and technical literacy and, accordingly, less likely to have a DFS account. DFS transaction errors are among the most common reasons for monetary loss in DFS (Wechsler, M., & Siwakoti, S., 2022). The familiarity of women with such disappointment suggests that they might be more sympathetic to others with the same issue, possibly increasing their susceptibility to transaction reversal fraud (Wechsler, M., & Siwakoti, S., 2022). Women must also be cautious about money and financial information which may be visible on shared mobile phones, such as vouchers and cash balances, which other family members may discover and claim for themselves (Wechsler, M., & Siwakoti, S., 2022). As a result, unbanked and underserved women may have a tendency to be more cautious and risk averse than men (Wechsler, M., & Siwakoti, S., 2022).



Women who lose money through DFS – victims of cybersecurity failures, capacity limitations or DFS fraud – can face notable derision (Wechsler, M., & Siwakoti, S., 2022). They may be blamed, shamed and ridiculed by family members, friends and even authorities (such as DFS agents, DFSP customer support representatives and police) even when it may not be their fault (Wechsler, M., & Siwakoti, S., 2022). This can diminish a woman's confidence in DFS, her abilities and her capacity for dealing with the consequences of failure as feelings of anticipated regret arise in advance of engaging in transactions (Wechsler, M., & Siwakoti, S., 2022). These reactions are reasons some posit that women are more likely to be more risk averse than men regarding situations where security could be compromised and risk of monetary loss are in issue (Wechsler, M., & Siwakoti, S., 2022).

Women that utilize frontline DFS services that are situated in strategic locations across rural areas are likely to experience over the counter fraud as well. One common over the counter fraud occurs when customers will give money to agents to conduct a transaction, but while the agent notifies the customer that the transaction has been completed, the customer does not receive a confirmation message and the party on the receiving end denies the transaction (Wechsler, M., & Siwakoti, S., 2022). Agents may extract their own premiums from customers for providing over the counter transactions (Wechsler, M., & Siwakoti, S., 2022). Customers may not be fully aware of the fees charged by agents nor that such practices are impermissible in various jurisdictions (Wechsler, M., & Siwakoti, S., 2022).

Another common over the counter fraud is unauthorized use of customer's PIN or transaction code. As the customer PIN is the doorway into accessing customer accounts, it is a popular target – especially since customers may be trusting in agents for assistance and don't fully appreciate the nature of the circumstances and critical need for protection (Wechsler, M., & Siwakoti, S., 2022). Unscrupulous agents may try to obtain a customer PIN for later unauthorized use or do so when freely given to them for assisted transactions, which is common (Wechsler, M., & Siwakoti, S., 2022). They may also try to convince customers that a first transaction was unsuccessful and to repeat it a second time, ultimately providing the customer with funds for one transaction when two actually occurred (Wechsler, M., & Siwakoti, S., 2022). As for the unauthorized use of customer transaction code; an agent may inform a customer that the use of a transaction code for withdrawing funds was unsuccessful, only to be used later by an agent at another location (Wechsler, M., & Siwakoti, S., 2022).

Finally, split transactions or imposition of illegal customer charges, tips, fees take place over the counter. Agents may pressure customers to split transactions into smaller amounts, such as not having sufficient cash on hand for withdrawals, so that they can generate greater commissions (Wechsler, M., & Siwakoti, S., 2022). In addition to this, agents may pressure customers to provide them with tips, charge them bogus or higher transaction fees, especially the case with illiterate customers (Wechsler, M., & Siwakoti, S., 2022).

# Sexual Harassment

Harassment of women may present a notable deterrent to their use of and familiarity with ICT and DFS, reducing financial, technical and cybersecurity knowledge and experience (Wechsler, M., & Siwakoti, S., 2022). Customer onboarding and GRM requires women to provide private information, phone numbers, photographs (for KYC, sometimes GRM); a disproportionate and predominantly male representation of agents or employees may increase risks of information disclosure and sexual harassment, especially in jurisdictions lacking adequate cyber law and regulation (Wechsler, M., & Siwakoti, S., 2022). Women in Bangladesh have shared concerns about personal and contact information shared during DFS onboarding and in agent assistance (Wechsler, M., & Siwakoti, S., 2022). Once onboarded, many also reported experiencing some form of sexual harassment when using DFS and receiving such phone calls from unknown men (Wechsler, M., & Siwakoti, S., 2022). Employees and officials in the police force and resolution processes of several South Asian countries are predominantly male, thus reporting fraud or harassment claims to the police often involves leaving personal information and an experience with authorities which women generally lack trust (Wechsler, M., & Siwakoti, S., 2022). The same trend could also be found in developing African countries.



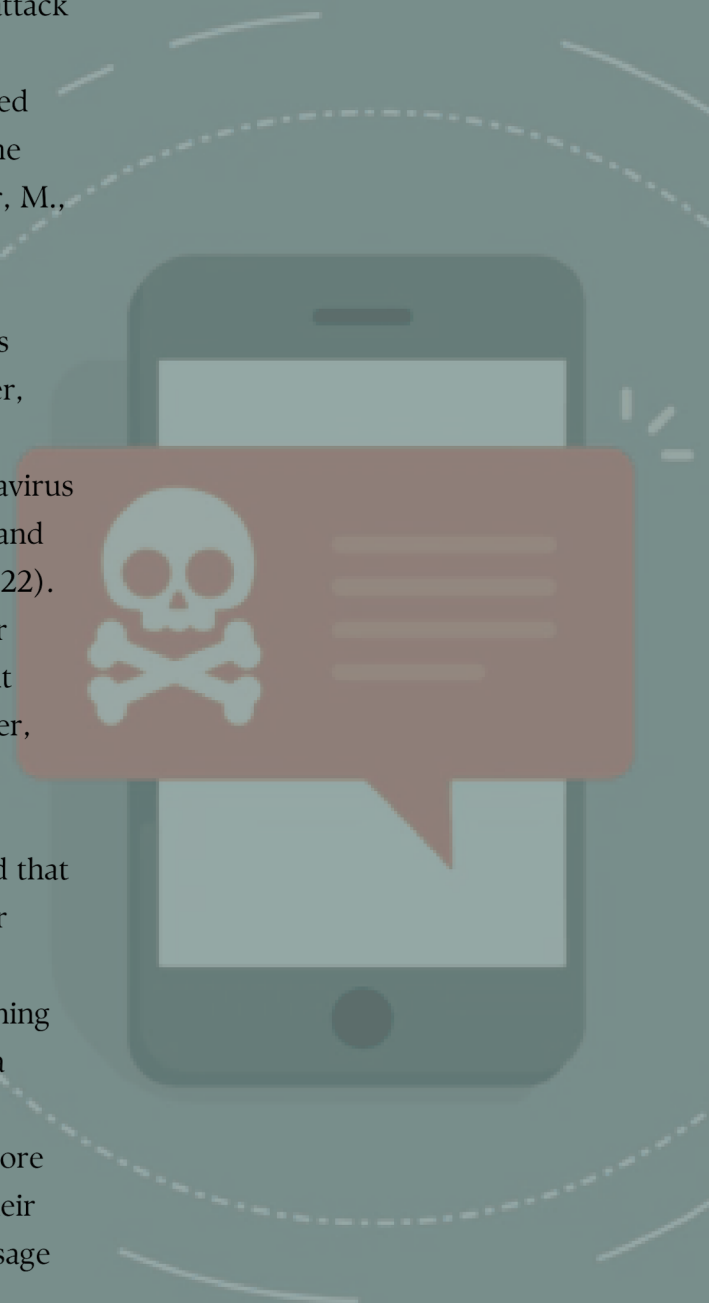


# Smishing

Smishing (sometimes appearing as “SMiShing”) is an SMS-based social engineering attack that is highly popular in developing countries since all mobile phones and accounts are capable of sending and receiving text messages (Wechsler, M., & Siwakoti, S., 2022). Like email phishing, smishing can be efficient, scalable, cost-effective, automated and capable of bulk messaging, with campaigns designed to reach the maximum number of victims with a minimum time invested (Wechsler, M., & Siwakoti, S., 2022). SMS messaging can be an ideal attack as text messages have, in comparison to other mediums of communication, the highest open/read rate; are often viewed quickly; have a high response rate; and inherently exhibit the urgency factor which can increase success rates (Wechsler, M., & Siwakoti, S., 2022).

In the shadow of Safaricom announcing its independent funding efforts to fight the COVID-19 pandemic, fraudsters engaged in a pervasive and timely smishing scam (Wechsler, M., & Siwakoti, S., 2022). Text messages were sent to consumers about purported, non-existent Safaricom coronavirus offers such as cash relief assistance payments, free airtime and free Internet data offers (Wechsler, M., & Siwakoti, S., 2022). These campaigns induced victims to “verify” their customer status by texting their PIN numbers, passwords and account numbers to a number controlled by the fraudster (Wechsler, M., & Siwakoti, S., 2022).

Industry experts and central banks we interviewed reported that while the pandemic had not been a source of inspiration for creating entirely new types of smishing fraud, there was a noticeably increased volume of occurrence, especially smishing scams (Wechsler, M., & Siwakoti, S., 2022). Additionally, a small study of professionals in Ghana also yielded a greater volume of smishing attacks than vishing, with men being more susceptible to mobile-based vulnerability stemming from their risk-taking nature and abundance of comfort with online usage (Wechsler, M., & Siwakoti, S., 2022). A 2018 consumer protection survey in Ghana (Ghana CP Survey) yielded relevant results relating to attack vectors and DFS scams, with participants reporting the following victimization rates: 29% by smishing and vishing attacks; 50% receiving transfer reversal requests with lower income persons being 19% more likely to be victimized by a scam (Wechsler, M., & Siwakoti, S., 2022).



# Phishing





Phishing is generally understood as the process of casting lures using Internet e-mail to deceive recipients into disclosing sensitive information or providing access to a secured environment, often accomplished by inducing the recipient to click on a hyperlink (Wechsler, M., & Siwakoti, S., 2022). Mobile phones represent ideal hardware for phishing frauds due to the fact that they are portable, often carried by and instantly accessible to users, and data is often adapted and abbreviated to fit small screen sizes which can hide important details and confuse users such as URLs hidden or abbreviated and conceal URL and domain spoofing (Wechsler, M., & Siwakoti, S., 2022). There exists a myriad of phishing definitions, which is frequently used as an umbrella term to describe the attack mechanism in several vectors (Wechsler, M., & Siwakoti, S., 2022). Along with pretexting scams, SMS and voice phishing are often used to defraud people in developing countries using basic and feature phones (Wechsler, M., & Siwakoti, S., 2022). Many phishing attacks, especially smishing and which is common in DFS, often consists of two stages (Wechsler, M., & Siwakoti, S., 2022):

(i) a bad actor who masquerades as a legitimate party who communicates a message to the victim with a call to action (ii) which is intended to elicit an expeditious or urgent response by the victim. Time limited or urgent communications are designed to divert the user's attention away from noticing specific message details that would indicate its deceptive nature and towards a compelling need for urgency in responding – such as to avoid missing out on the collection of a valuable reward. The concept of urgency is one of several “influence techniques” commonly used to effectuate social engineering scams in the context of DFS. A select list includes (Wechsler, M., & Siwakoti, S., 2022):

- Authority-The tendency of people to follow messages sent by a recognizable authority;
- Reciprocity- The tendency for people to feel obligated or eager to return favors;
- Social Proof- The tendency of people to comply with or feel that an opportunity is safe when it is implied others have participated safely;
- Sympathy- The natural inclination people may have to assist those in need.
- Scarcity/Reward- The tendency of people to comply or respond to communication when there is a belief that a rare opportunity may exist;
- Urgency- The tendency of people to act when presented with a limited time to potentially obtain a benefit or to avoid a loss. These influence techniques have been used to create several popular social engineering frauds which have become prevalent in developing countries and affect DFS customers.

# Vishing



Vishing uses the telephone voice channel to commit social engineering scams (Wechsler, M., & Siwakoti, S., 2022). In its simplest form, fraudsters may call random consumers directly, often posing as an authority to effectuate fee scams and disclosure frauds (Wechsler, M., & Siwakoti, S., 2022). Scalability is improved by solicitation of consumers (such as posing as a recognized authority) via SMS distribution containing a phone number for recipients to reply (Wechsler, M., & Siwakoti, S., 2022). Robocalling may also be used, in conjunction with Voice Over Internet Protocol (VOIP), to “spoof” originating telephone numbers, making the caller appear to have a familiar or local number (Wechsler, M., & Siwakoti, S., 2022). Integrated voice recognition (IVR) systems can also be used to refine the efficiency of the fraud (Wechsler, M., & Siwakoti, S., 2022). Victims call a designated number and are prompted to navigate through a purported support system, eventually leaving messages as instructed which include PIN and other requested information to assist with the “verification” of their account (Wechsler, M., & Siwakoti, S., 2022). As with smishing, very few relevant vishing studies related to developing countries were located (Wechsler, M., & Siwakoti, S., 2022).

# Pretexting / Impersonation



Pretexting attacks consist of creating a phony, contrived scenario to convince an unsuspecting person to trust the attacker and follow a requested directive, such as divulging sensitive and/or confidential information (Wechsler, M., & Siwakoti, S., 2022). Common examples include a fraudster posing as an authority such as an MNO or DFSP support representative or outside consultant (Wechsler, M., & Siwakoti, S., 2022). While pretexting may be categorized separately, it is often closely connected with a phishing, smishing or vishing attack (Wechsler, M., & Siwakoti, S., 2022). Pretexting is often distinguished from other types of mass attack methods, such as email phishing, in its more elaborate effort to convince victims beyond the ephemeral “cast and catch” nature of phishing attacks (Wechsler, M., & Siwakoti, S., 2022). Pretexting focuses predominantly on creating trust and building a rapport with the victim to win their confidence, in contrast to preying on a momentary sense of urgency of the victim to respond that is characteristic of phishing attacks (Wechsler, M., & Siwakoti, S., 2022).



# Frauds



Anecdotal evidence and some relevant studies loosely suggest that unbanked and underserved women in Africa and South Asia may exhibit tendencies to be more compliant with authority and sympathetic towards others and more risk averse than men. Men were observed to be victimized more often by advance fee and lottery scams. It is important to note that results can vary within different regions, population demographics, cultures, and other factors comprising this complex subject. Frauds that will be discussed in this section use similar strategies to the other scams mentioned above. Repeated attacks are made to induce relatively small payments from victims, profiting through transaction volume (Wechsler, M., & Siwakoti, S., 2022). The amounts requested are sufficiently modest to fall under levels which would raise internal alarms and likely to be dismissed by victims after discovery due to the considerable investment and effort necessary to pursue a potentially unsuccessful remedy (Wechsler, M., & Siwakoti, S., 2022). The most common forms of these theft of funds include the following (Wechsler, M., & Siwakoti, S., 2022):

**Advance Fee Scams.** A victim is lured by an ostensible opportunity to receive a considerable gain by remitting a much smaller amount – an advance fee – to preserve an opportunity or to effectuate the transfer of a non-existent windfall. Common schemes include the victim receiving notice of winning a lottery, prize, loyalty benefit from an Mobile Network Operator (MNO) or DFSP or a package sent from a relative or vendor. In each of these examples some type of small advance fee is required to be paid by the victim, such as a modest deposit or processing and/or shipping fee.

**Purported Wrong Transfer.** A fraudster transmits a fake money transfer notification to the victim, usually via SMS. It is followed by a subsequent message explaining that the transfer was sent in error to the wrong customer number with a request for remittance back of the funds. Impulsively, the victim may remit money to the sender without a prior review and confirmation that a transaction had actually occurred. Results reported in the IFC Bangladesh Study numbers suggest that women might be more susceptible to being victimized by this scam than men.

**Assistance or Sympathy Scam.** The fraudster communicates an emotional plea for an urgent transfer of funds to assist the sender or the sender's family member in a dire situation, such as for urgently needed medical care. The message can take the form of a purported wrong transfer (e.g. money was sent money to the wrong account, intended for the hospital); or purportedly from a friend in need (impersonation); or from a stranger in need of a good Samaritan, preying on the goodwill and nature of the victim who receives the plea.

**Extortion Scam.** The fraudster informs the victim that they will be harmed in some fashion unless they remit a payment. In the context of gender, this often translates into a threat to reveal sensitive private details, e.g. knowledge or photos relating to an embarrassing incident, etc.

Identity fraud or identity theft occurs when such disclosed information can be used for personal identification purposes to impersonate the victim. This is often a precursor to a subsequent act which uses the data to commit one or more financial frauds. DFS customers are commonly duped into disclosing their PIN and other sensitive information by fraudsters posing as MNO representatives seeking to "confirm" the subscriber's identity to provide them with a special award, upgrade or in response to technical support pretexts.

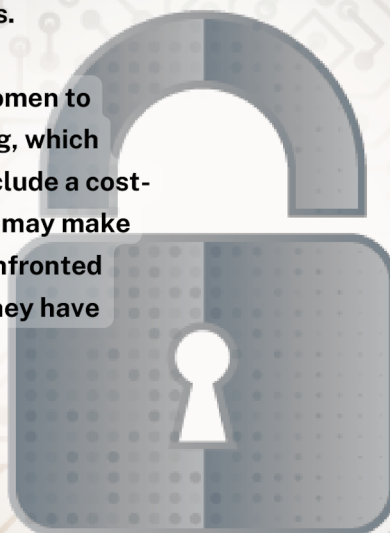
SIM swap fraud is a pervasive global problem, especially in developing countries where DFS customers are poor and have virtually no loss tolerance. Large scale attacks are occurring in developing countries, including South Africa where reported attacks doubled in one year. The largest bank in Mozambique reported over 17 average SIM-swap frauds each month. Sometimes fraudsters can obtain sensitive customer information with a fraudster resulting from collusion with internal MNO employees, which has been a visible problem. SIM Swaps and Account Takeovers is a common type of MNO fraud where swapping out defective SIMs for customers takes place. SIM swap fraud occurs when an MNO is convinced to switch a customer's service to a SIM card possessed by a fraudster, often by a fraudster using a PIN code or other sensitive information obtained through identity theft to impersonate the customer. After seizing the customer's mobile account, the fraudster can siphon funds, airtime and value from that account as well as all linked accounts, and potentially apply for credit or other services using the identity of the victim. Social engineering techniques can also be used to exploit vulnerabilities in the two-factor authentication (2FA) process to effectively hijack a user's account. Recently, Safaricom launched its "Tuwaanike" service to combat SIM swap fraud which provides additional notification and an ability for subscribers to opt out of any unknown SIM swap requests.



# Recommendations

To face the issue of cybercrimes committed against women in Africa and South Asia researchers, Michael M. Wechsler and Samikshya Siwakoti recommended that (Wechsler, M., & Siwakoti, S., 2022):

- The increased penetration of ICT and DFS in developing countries mandate greater initiatives and efforts at capturing and sharing ICT, DFS and cybersecurity related data. Attention should be given to prioritize the capture and sharing of gender disaggregated data at data collection points as a general practice. Industry may serve as a driver for this initiative.
- Concerted efforts should be made to raise the level of cyber awareness and hygiene in DFS countries. These include those made by MNOs and DFSPs at time of onboarding as well as subsequently. Industry and government should supplement these efforts, which also needs to incorporate an initiative at the grassroots level in order to be effective.
- Continued reduction of social and cultural gender gaps to hopefully meaningfully reduce DFS and technology divides. Women's confidence and capacity levels in using DFS and ICT are an important driver towards their adoption and use and investment in learning cybersecurity best practices.
- Regions which exhibit substantial gender representation divides among DFS related personnel, such as agents and GRM representatives, should consider the initiatives of and efforts made by the Bank of Bangladesh and others, such as female agent recruitment and training programs.
- Greater emphasis and efforts should be made to encourage women to seek cyber and consumer fraud related assistance and reporting, which could increase women's confidence in the system. Examples include a cost-free hot line or reporting pipeline and/or text messaging, which may make women in rural areas less reluctant to seek assistance when confronted with ICT or DFS related knowledge gaps or when they believe they have been or might be exposed to fraud.





- Efforts should be made at improved tracking of smartphone adoption and usage. While the data indicates increasing smartphone penetration, research also revealed that what is considered a smartphone can noticeably lag behind the curve in terms of quality and performance. Network coverage and power/charging availability also create challenges, but the time would appear ripe to prioritize the creation and capture of a richer data set which would include gender disaggregation, security and usage trends.

- Women's encouragement and participation in STEM study and careers should be an important priority in developing countries. In rural areas, additional efforts should be made to increase basic financial and digital literacy levels.

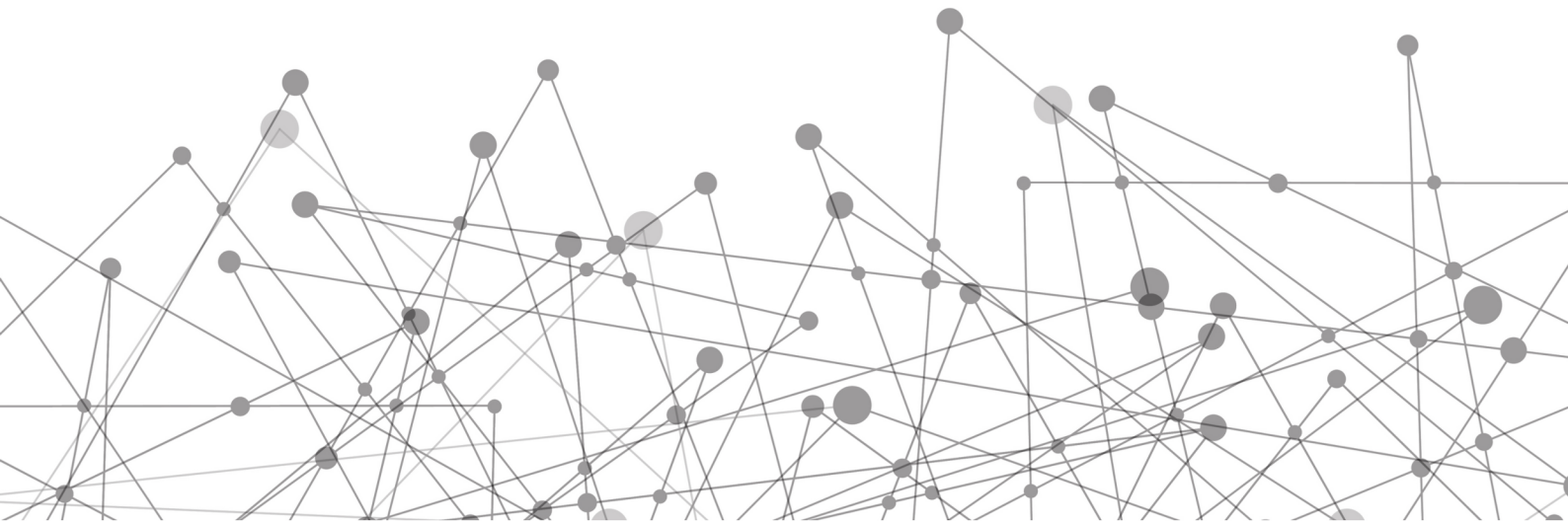
- Policy makers, regulators and financial services providers should consider increasing efforts towards an inclusive approach of "gender centrality" to ensure that gender-specific needs are addressed. This would appear to be of greater importance as it relates to ICT and mobile communications, an area where there is a notable gender divide which is more pronounced in rural areas. Trust in financial systems and the technology which drives the process is the mainstay of user adoption. Yet we have found that there are significant gender gaps relating to access to information, education, and ICT which lead to lower levels of digital capacity, technical literacy and, logically, reduced fraud and cyber awareness. The distinct lack of quantitative and qualitative research on cybersecurity as well as gender differences – such as overall level of cyber awareness and hygiene, susceptibility to fraud, social engineering and cyber-attacks – compels the need for additional focus, funding and attention to address this important issue by academic institutions, donor communities and think tanks.

# References

Microsoft. (n.d.). Bing. <https://www.bing.com/visualsearch>

Mountrouidou, X., Vosen, D., Kari, C., Azhar, M. Q., Bhatia, S., Gagne, G., Maguire, J., Tudor, L., & Yuen, T. T. (2019). Securing the Human: A Review of Literature on Broadening Diversity in Cybersecurity Education. *Proceedings of the Working Group Reports on Innovation and Technology in Computer Science Education*, 157–176. <https://doi-org.libproxy.udayton.edu/10.1145/3344429.3372507>

Wechsler, M., & Siwakoti, S. (2022, May 11). *Gender, Cybersecurity & Fraud*. SSRN. [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=4103747](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4103747)



---

## GENDER TECH INITIATIVE

Women & Cybersecurity: Investigating cybercrimes against women in the continent of Africa stemming from gender inequalities, and identifying strategies to combat this phenomenon.

<https://www.genderinitiativeug.org/>  
[info@genderinitiativeug.org](mailto:info@genderinitiativeug.org)  
+256 772 946 313