CYBERCRIME COUNSELING BY MAXIMIZING 2-FACTOR AUTHENTICATION (2-FA) FEATURES IN SEBATANG, KULON PROGO

Zalfa Nadira
UIN Sunan Kalijaga, Yogyakarta
zalfandr.12@gmail.com

Abstract - *The need for computer network technology in Indonesia today is growing. Technology plays a role as a media provider of information, as it unleashes the activities of the commercial community into the largest and fastest part of its growth as well as across national borders. This network is capable of moving market activity around the world and is known for 24 hours. Through the world of the Internet called cyberspace, anything can be done. The advancement of Internet technology has led to the emergence of "Cybercrime" or crimes through the Internet, including theft of credit cards, hacking several sites, intercepting the transmission of other people's data, such as emails, and manipulating data by preparing unwanted commands into computer programs. This phenomenon of cyber crime development needs to be anticipated by the younger generation so that they do not become perpetrators or victims. Therefore, make a judgment against the members of the Karang Taruna Arben in Sebatang, Kulon Progo. The methods used are observation, interactive exposure, simulation, as well as discussion. The expected outcome of this investigation is increased awareness of the cybercrime that is currently occurring.*

Keywords: *Counseling, Cyberspace, Cybercrime, Social Media, Communication Media*

1. INTRODUCTION

The advances in science and technology that humankind enjoys today in various parts of the world are one of the positive effects of globalization. The presence of a variety of sophisticated communication tools makes it easy for the world to acquire information quickly and connect each other with just one touch. The variety of information technology in digital form is becoming increasingly popular and in demand by the world community. Publicly, cyberspace known as the Internet has become a friend of everyday life, which then not only brings benefits but also threatens the security and rights of its users. (Simatupang & Ridwan, 2022)

The development of society is now an era of industrialization, as well as supported by the development of telecommunications technology, then the relations between nations are already worldwide which then creates a new world order. (Habibi & Liviani, 2020) The Internet is one aspect that is undergoing very rapid development. The Internet has become one of the obligations in life today. (Gani, 2020) That fact also affects the development of crime. There have been a lot of cybercrime cases in Indonesia, ranging from identity fraud to debt bill terror that never even happened. These cyber-crimes are done through social media, such as Facebook, WhatsApp, Instagram, and more.

It is said that a citizen in the district of Sebatang has experienced online fraud via WhatsApp. This crime mode is a wedding invitation message but the format used is APK. This has been watched by various parties, it is due to the download of the file then the WhatsApp account used will be hacked and all the information in the phone will also hacked.

In order to anticipate the recurrence of social media fraud against the citizens of Sebatang, a cybercrime investigation was conducted accompanied by the maximization of 2-Factor Authentication (2-FA) features. Based on the experience of the incidents that have affected one of these citizens, it is not expected that something similar will happen to other citizens with vigilance against the cyberspace.

2. METHOD

Research methods of interactive exposure, simulation, and discussion are methods used in research to obtain data, understanding, or research results using an approach that focuses on communication, interaction, and participation between researchers and respondents or research participants. Here is the definition of each method: (Andi, 2012)

a) Observation
Data collected through observation is usually a description of behavior or events observed. Researchers then analyze this data to identify patterns, trends, or findings that are relevant to the purposes of the research. Analysis of observational data can involve qualitative or quantitative methods, depending on the research approach used.

b) An interactive exhibition
   An interactive exhibition is a research method in which researchers communicate research information or material to respondents or research participants through live presentations or interactive media such as multimedia, computer-based presentations, or practical demonstrations. Interactions between researchers and respondents usually occur during or after exposure to obtain responses, questions, or further understanding.

c) Simulation
   Simulation is a research method in which a particular situation or condition is artificially replicated to allow respondents or study participants to interact with the situation without any real risk. Simulation can be used in a variety of contexts, such as educational research, medical research, or management research, to understand individual reactions, decisions, or performance in controlled situations.

d) Discussions
   Discussions are research methods that involve verbal or written communication between researchers and respondents or between respondents themselves. The purpose of the discussion is to gather qualitative data, understand the perspectives, experiences, or views of respondents, and enable interaction and exchange of ideas between them.

These methods can be used simultaneously or separately depending on the purpose of the research, the context, and the type of data to be obtained. The selection of appropriate research methods should be adapted to the research questions and the research framework used.

A. Tools and materials

Tools and materials used:

1) Powerpoint (material socialization of the investigation of cybercrime by maximizing of 2-Factor Authentication)
2) Proyector
3) Laptop
4) Handphone

B. Work procedures

In this study were carried out in 4 stages:

1) Observation
   Observation of this stage, performed observation of the cybercrimes problems through the marks of online corruption and conducted an interview with Mrs. Asih Suprapti as a manager Karang Taruna Arben and as an advisor to hold socialization related to cybercrime.
2) An interactive exhibition

In this phase, literacy research is carried out through books and the Internet on the definition, examples, ways of working, and solutions to material cybercrime. A way to compile the drafting material to be more interactive is to use PowerPoint media. Thus, the more trans procession of science is expected to be more attractive and well-reviewed by the participants.

3) Simulation

   Simulation in this stage is meant to be 2-Factor Authentication (2-FA) practice. In its own action, two students will explain through PowerPoint media and eight students will accompany the participants if there are obstacles or anything questionable in the process.

4) Discussions

   The discussion are carried out at the final stage of socialization. It includes question-and-answer activities and discussions.

3. RESULTS AND DISCUSSION

The term "cybercrime" refers to a criminal act related to cyberspace and digital-based crime. There are experts who equate cybercrimes with computer crimes and there is an expert who distinguishes between the two. Cybercrime is an attempt to enter or use a computer facility or computer network without permission and against the law with or without causing alteration and/or damage to the computer facilities entered or used.

Wisnubroto (1999) defines cybercrime as an act against the law committed by using the Internet as a means/tool/object, whether to gain or not, to the detriment of others. (Muthia & Arifin, 2019)

Cybercrime is one of the dark sides of technological advances that has a very outward negative impact on the whole area of modern life today. Concerning concerns about the dangers of cybercrime, as they are closely linked to “economic crime” and “organized crime” (especially for the purposes of “money laundering”). (Habibi & Liviani, 2020)

The cyberspace is more vulnerable due to a variety of factors, including the increasingly difficult security systems to access, gaps in hacking, and the level of personal data leakage. Social media does have many advantages like fast access, easy, and cheap, but understanding digital literacy, is less. (Haryanto, 2016)

The cyber activity, although virtual, can be categorized as a real act of law. Juridically, in the case of cyberspace, it is no longer in place to categorize something with the measure in the qualification of conventional law to be an object and act, because if this method is used, there will be too many difficulties and things will escape the legal trap. (Wahyudi et al., 2022) Cyber activity is a virtual activity that has a very real impact, even though the evidence is electronic. Thus, the subject of the offender must be qualified as the person who has committed a manifest act of law (Takanjanji, 2020).

Forms of cybercrime: (Handayani et al., 2023)

1. Phising
   Theft by stealing important information by directing the victim to enter a fake page/site aimed at trapping the victims. Typically, these crimes target paid streaming services, banking, e-commerce, and a small company.
2. Scam
   Is a fraud that usually aims to earn money by sending messages with sentences of coercion or intimidating a victim.
3. Account Takeover
   Is a sudden account takeover fraud and the victim usually feels the impact in an instant.
4. Social Engineering
   Is misconduct by deceiving a victim or manipulating the victim's psychology to unconsciously provide his personal information. It's usually done through fake sites, texting, social media, and over the phone.
5. Share Login Info
   Is a fraud by stealing sensitive account information (PIN, OTP, and password).
6. ID Theft
   Is a fraud with the stealing of a victim's identity card. The identity is then used to register an account on a platform with the identity of another person.
7. Skimming
   A fraud in which the victim's personal information in an electronic card (such as a credit card) is taken through a tool that is secretly embedded in a card reader.
8. Pharming
   Means that the victim receives an email from a certain source convincing them, that it has won a prize and in order to get the prize, the victim must reply to the email with certain information.
9. Scareware
   Is an intruder program designed to trick users into buying and downloading various malicious software such as fake antivirus.

The cybercrime investigation activity with maximization of 2-Factor Authentication (2-FA) features in Sebatang, Kulon Progo was attended by members of Karang Taruna Arben as many as 25 people. Followed this investigation was a digital literacy emergency against technology users, the scourge of cybercrimes, and the incident that struck one of the citizens in Sebatang, Kulon Progo, becoming a victim of online fraud. The exhibition was conducted by two students and the simulation was accompanied by eight students of the Kuliah Kerja Nyata (KKN) from UIN Sunan Kalijaga, Yogyakarta.

Figure 1. Documentation of socialization of cybercrime counseling

In line with the purpose of this design, is maximizing the 2-Factor Authentication (2-FA) feature, simulations and implementations were carried out on three social media sites. (WhatsApp, Instagram, and Facebook).

Because there are so many attackers who take private information and take over an account. The company provides 2-FA features to secure accounts from third parties who want to access user accounts. The 2-FA concept not only requires users to enter usernames and passwords but also OTP codes sent via message or email.

1. WhatsApp

   2-Factor Authentication (2-FA) is an optional feature that adds more security to your WhatsApp account. You'll see the 2 Factor Authentication (2-FA) screen after you successfully register your phone number on WhatsApp. Learn how to enable 2-Factor Authentication (2-FA) in this article.

   When you enable 2-Factor Authentication (2-FA), you can enter your email address. This helps to safeguard your account by allowing WhatsApp to email you a reset link if you ever forget your PIN, and email you a verification code when you register your account. How to register using an email verification code:

   a) Check that your phone has a strong internet signal.
   b) Open WhatsApp and follow the steps to begin registering your phone number on Android or iPhone.
   c) You'll receive a 6-digit registration code via email once you enter your phone number.
      - Note: This will only happen if you've set up 2-Factor Authentication (2-FA) and have previously added your email address. You'll receive a prompt to check your email and enter the code.

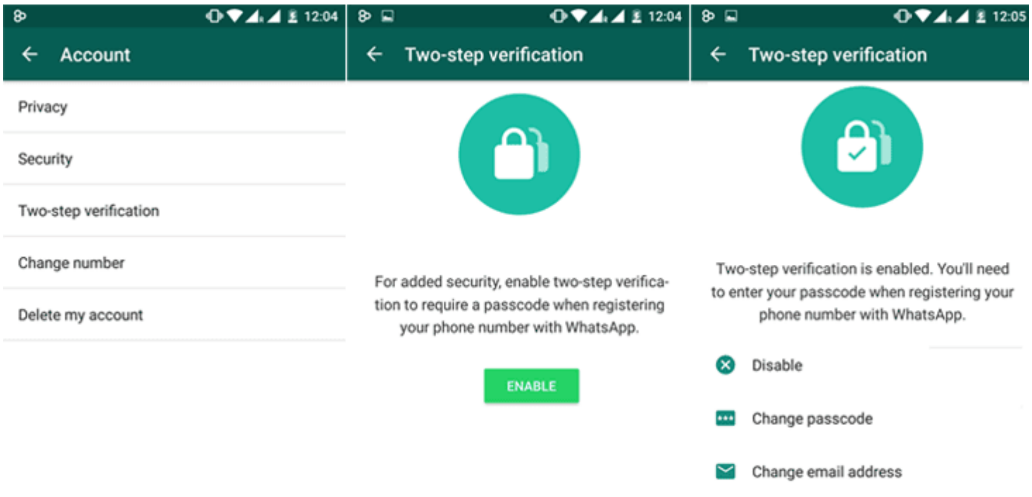
- If you don’t receive your code, you can request a new one by email, SMS or phone call.
- Note: Depending on your carrier, you may be charged for SMS and phone calls.

d) Enter your 6-digit code to complete registration.

Reset your two-step verification PIN. If you provided an email address when you set up 2-Factor Authentication (2-FA), you can reset the PIN by requesting a new one via SMS. To reset the PIN:

- Android: Open WhatsApp > tap Forgot PIN? > Send code > enter the six digit code sent to your registered phone number.
- iPhone: Open WhatsApp > tap Forgot PIN? > Send Code > enter the six digit code sent to your registered phone number.

Note: If you don’t receive your code, tap Didn’t receive a verification code? and request a new code by email, SMS or phone call. (*About Email Verification Codes and Resetting Two-Factor Authentication | WhatsApp Help Center*, n.d.)



For added security, enable two-step verification to require a passcode when registering your phone number with WhatsApp.

Two-step verification is enabled. You'll need to enter your passcode when registering your phone number with WhatsApp.

Figure 2. WhatssApp 2-FA

2. Instagram

2-Factor Authentication (2-FA) protects your account by requiring a code if there’s a login attempt from a device we don't recognize.

To turn on 2-Factor Authentication (2-FA):

a) Click menu More in the bottom left, then click Settings.

b) Click Privacy and Security from the menu on the left.

c) Scroll down to 2-Factor Authentication (2-FA), then click Edit 2-Factor Authentication (2-FA) setting.

d) Choose the security method you want to add and follow the on-screen instructions.

When you set up 2-Factor Authentication (2-FA) on Instagram, you’ll be asked to choose one of three security methods:

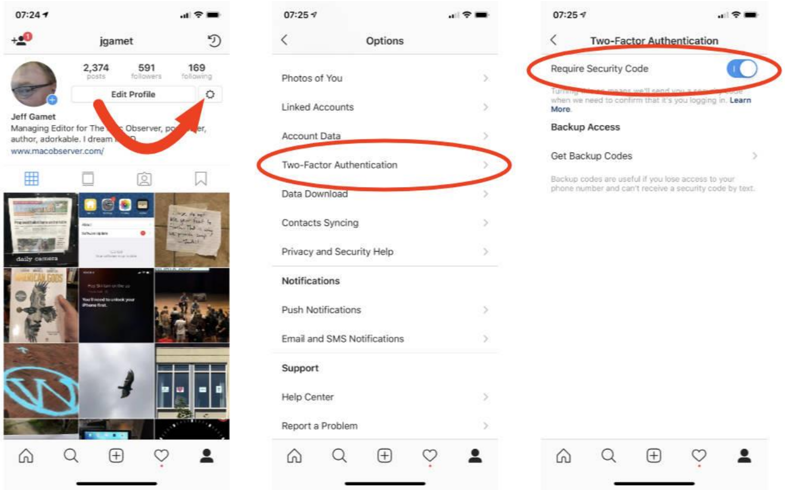
- Authentication app: (recommended): Download an authentication app, such as Duo Mobile or Google Authenticator to get login codes. This security method is recommended, because you can add multiple devices connected to an account so they can all get login codes. Note: 2-Factor Authentication (2-FA) through an authentication app can only be turned on using the Instagram app for Android and iPhone.
- Text message: We'll send a login code to your mobile number.
- WhatsApp: Turn on the text message security method first. Then, you can turn on the WhatsApp security method to get login codes from WhatsApp.

You'll need to have at least one of these set up in order to use 2-Factor Authentication (2-FA).

Note: After you've turned on 2-Factor Authentication (2-FA), you'll be able to see login requests and remove trusted devices. If you lose access to your phone or email address and are unable to get login codes, you can use a backup code to log in. Learn more about login codes.

Keep in mind that:

- If you haven't marked the device you're using as a trusted device, you can do so when you log in from that device using 2-Factor Authentication (2-FA). This way you won't have to enter a security code when you log in again. Trusted devices are any device that you've already signed in to using 2-Factor Authentication (2-FA) and have marked as trusted by tapping Trust this device.
- You shouldn't tap Trust this device if you're using a public or shared device that other people you may not know can access.
- To set up text message (SMS) 2-Factor Authentication (2-FA), you can either use a mobile number that's already been added to your account or add a new number. (*Securing Your Instagram Account with Two-Factor Authentication | Instagram Help Center*, n.d.)



Backup codes are useful if you lose access to your phone number and can't receive a security code by text.

Figure 3. Instagram 2-FA

3. Facebook

2-Factor Authentication (2-FA) is a security feature that helps protect your Facebook account in addition to your password. If you set up two-factor authentication, you'll be asked to enter a special login code or confirm your login attempt each time someone tries accessing Facebook from a browser or mobile device that we don't recognise. You can also get alerts when someone tries logging in from a browser or mobile device that we don't recognise. Turn on or manage 2-Factor Authentication (2-FA):

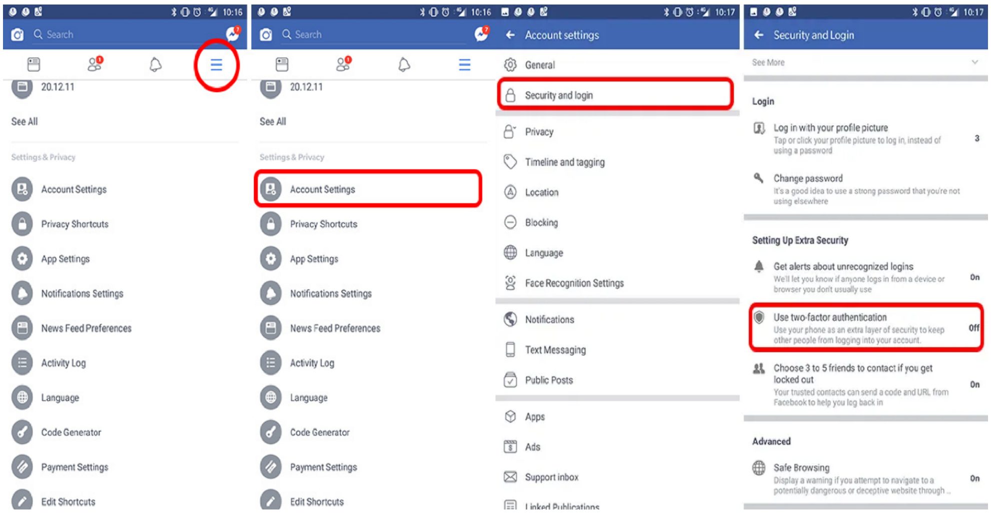
a) Go to your Security and login settings.
b) Scroll down to Use 2-Factor Authentication (2-FA) and click Edit.
c) Choose the security method that you want to add and follow the on-screen instructions.

When you set up 2-Factor Authentication (2-FA) on Facebook, you'll be asked to choose one of three security methods:

a) Tapping your security key on a compatible device.
b) Login codes from a third-party authentication app.
c) Text message (SMS) codes from your mobile phone.

Once you've turned on 2-Factor Authentication (2-FA), you can get ten recovery login codes to use when you're unable to use your phone. Learn how to set up recovery codes. Other useful resources:

- If you haven't saved the browser or mobile device that you're using, you'll be asked to do so when you turn on 2-Factor Authentication (2-FA). This way, you won't have to enter a security code when you log in again. Don't click Save this browser if you're using a public computer that other people can access (e.g. a library computer).
- We need to be able to remember your computer and browser information so that we can recognise it the next time you log in. Some browser features block this. If you've turned on private browsing or set up your browser to clear your history every time it closes, you might have to enter a code every time you log in. Learn more.
- To set up text message (SMS) 2-Factor Authentication (2-FA), you can either use a mobile number that's already been added to your account or add a new number. Learn more about how Facebook uses a mobile number added for 2-Factor Authentication (2-FA).
- Learn about what you can do if you turned on 2-Factor Authentication (2-FA) but are now having trouble with logging in. (*How Two-Factor Authentication Works on Facebook. | Facebook Help Centre*, n.d.)



Login

Log in with your profile picture — Tap or click your profile picture to log in, instead of using a password — 3

Change password — It's a good idea to use a strong password that you're not using elsewhere

Setting Up Extra Security

Get alerts about unrecognized logins — We'll let you know if anyone logs in from a device or browser you don't usually use — On

Use two-factor authentication — Use your phone as an extra layer of security to keep other people from logging into your account. — Off

Choose 3 to 5 friends to contact if you get locked out — Your trusted contacts can send a code and URL from Facebook to help you log back in — On

Advanced

Safe Browsing — Display a warning if you attempt to navigate to a potentially dangerous or deceptive website through ... — On

Figure 4. Facebook 2-FA

Some tips to bear in mind against social media users, among others:

1. Use unique passwords
2. Change passwords on a regular basis
3. Beware of strangers' calling
4. Don't access suspicious links unwittingly.

4. CONCLUSION

Internet actually has a negative side in its development, as it opens up opportunities for cybercrime activities that were previously considered impossible to do and to be. According to the theory, evil is the product of society itself, which means that society itself creates evil. The phenomenon of cybercrime should be cautious as this crime is somewhat different from other crimes in general. Cybercrime can be committed without knowing the boundaries of the territory and does not require direct interaction between the perpetrator and the victim of the crime.

The cybercrime detection activities with maximization of 2-Factor Authentication (2-FA) features in Sebatang, Kulon Progo which have been carried out exactly on Saturday, August 5, 2023, are running well and smoothly. Participants consisting of members of Karang Taruna Arben are observed, responded, and followed simulation instructions using 2-FA features on 3 social media. (WhatsApp, Instagram, and Facebook). This disclosure is accompanied by simple tips for social media users.

In addition to providing advice and caution, this advice is expected to be one of the knowledge that will then be disseminated to the citizens of Sebatang, Kulon Progo in particular, and other citizens in general.

REFERENCE

About email verification codes and resetting two-factor authentication | WhatsApp Help Center. (n.d.). Retrieved September 2, 2023, from https://faq.whatsapp.com/1082491466048496/?helpref=search&query=factor%20atuhentication&search_session_id=bb0c8b5e843093c86463636c2b8b30b1&sr=0

Andi, P. (2012). Metode penelitian kualitatif dalam perspektif rancangan penelitian. *Ar-Ruzz Media*.

Gani, A. (2020). Cybercrime (Kejahatan Berbasis Komputer). *JSI (Jurnal Sistem Informasi) Universitas Suryadarma*, *5*(1), 16–29.

Habibi, M. R., & Liviani, I. (2020). Kejahatan Teknologi Informasi (Cyber Crime) dan Penanggulangannya dalam Sistem Hukum Indonesia. *Al-Qanun: Jurnal Pemikiran Dan Pembaharuan Hukum Islam*, *23*(2), 400–426.

Handayani, D., Rosianah, S. F., Sobari, D. I., Putra, D. A., Zulhija, H. M., Maulida, I., Agdana, M. A. P., Mubarakh, M. K., Wulansari, W., & Khanafi, W. F. (2023). Ragam Modus Cyber Crime Di Era Digital 4.0. *Abdi Jurnal Publikasi*, *1*(4), 422–427.

Haryanto, H. (2016). Pemanfaatan Social Media Network Sebagai Media Komunikasi Komunitas Pustakawan Homogen Dalam Rangka Optimalisasi Resources Sharing Koleksi Antar Perguruan Tinggi. *Pustakaloka*, *8*(1), 130–141.

How two-factor authentication works on Facebook. | Facebook Help Centre. (n.d.). Retrieved September 2, 2023, from https://www.facebook.com/help/148233965247823

Muthia, F. R., & Arifin, R. (2019). Kajian Hukum Pidana Pada Kasus Kejahatan Mayantara (Cybercrime) Dalam Perkara Pencemaran Nama Baik Di Indonesia. *RESAM Jurnal Hukum*, *5*(1), 21–39.

Securing your Instagram account with two-factor authentication | Instagram Help Center. (n.d.). Retrieved September 2, 2023, from https://help.instagram.com/566810106808145

Simatupang, H. Y., & Ridwan, R. (2022). Penyuluhan Dampak Cyber Crime Terhadap Keamanan Nasional Di Kalangan Pelajar MAS YASPI Labuhan Deli Medan. *PUBLIDIMAS (Publikasi Pengabdian Masyarakat)*, *2*(1), 160–168.

Takanjanji, J. (2020). Merefleksi Penegakan Hukum Tindak Pidana Penipuan Online. *Widya Pranata Hukum: Jurnal Kajian Dan Penelitian Hukum*, *2*(2), 75–90.

Wahyudi, D., Samosir, H. S., & Devi, R. S. (2022). Akibat Hukum Bagi Pelaku Tindak Pidana Penipuan Online Melalui Modus Arisan Online Di Media Sosial Elektronik. *JURNAL RECTUM: Tinjauan Yuridis Penanganan Tindak Pidana*, *4*(2), 326–336.