PENYULUHAN MENGENAI KEAMANAN DAN KEBENARAN INFORMASI DIGITAL SAAT PANDEMIK COVID-19

Fransiskus Adikara, Sandfreni, Putra Fajar Alam
Fakultas Ilmu Komputer, Universitas Esa Unggul
Jalan Arjuna Utara No. 9, Jakarta, Indonesia
fransiskus.adikara@esaunggul.ac.id

Abstract

Implementation of Community Service in the context of the Scientific Forum of Lecturers conducted jointly with the Research and Community Service Institute, Esa Unggul University, West Jakarta. This outreach program is intended for lecturers, educators, and other general participants who aim to share knowledge or transfer knowledge about the security and truth of digital information in today's special era during the Covid-19 pandemic. With this activity, the specific target to be achieved is so that participants can understand the concept of digital information security and be able to understand the truth of digital information that is currently circulating a lot. With this knowledge and understanding, especially for participants who are unfamiliar with digital technology, which in this pandemic period must follow the development of technology, it is hoped that they will gain the ability to maintain the security and correctness of their information. The method used is in the form of counseling with practical delivery through knowledge transfer and presentation of features and practical examples delivered online through a webinar event using the Zoom method. After the webinar event was finished, the participants filled out a questionnaire to get a conclusion on the knowledge transfer that had been carried out.

Keywords :digital information security, truth of digital information security, covid-19

Abstrak

Pelaksanaan Pengabdian Kepada Masyarakat dalam kerangka acara Forum Ilmiah Dosen yang dilakukan bersama dengan Lembaga Penelitian dan Pengabdian Masyarakat, Universitas Esa Unggul, Jakarta Barat.Acara penyuluhan ini diperuntukan untuk para dosen, tenaga pedidik, dan peserta umum lainnya yang bertujuan untuk berbagi pengetahuan atau *transfer knowledge* mengenai keamanan dan kebeneran informasi digital di zaman *now* khusus pada masa pandemic Covid-19. Dengan adanya kegiatan ini, target khusus yang hendak dicapai adalah agar para peserta dapat memahami konsep keamanan informasi digital serta dan berkemampuan untuk memahami kebenaran informasi digital yang saat ini banyak beredar. Dengan pengetahuan dan pemahaman ini, terutama bagi peserta yang awam akan teknologi digital yang di masa pandemik ini harus mengikuti perkembangan teknologi diharapkan mulai mendapatkan kemampuan dalam menjaga keamanan dan kebenaran informasi yang dimilikinya. Metode yang digunakan berbentuk penyuluhan dengan penyampaian yang praktis melalui transfer ilmu dan sajian ciri-ciri serta contoh praktis yang disampaikan secara daring melalui sebuah acara webinar menggunakan metode Zoom. Setelah acara webinar selesai dilaksanakan, para peserta mengisi kuesioner untuk mendapatkan kesimpulan atas *transfer knowledge* yang telah dilaksanakan.

Kata kunci: keamanan informasi digital, kebenaran informasi digital, covid-19

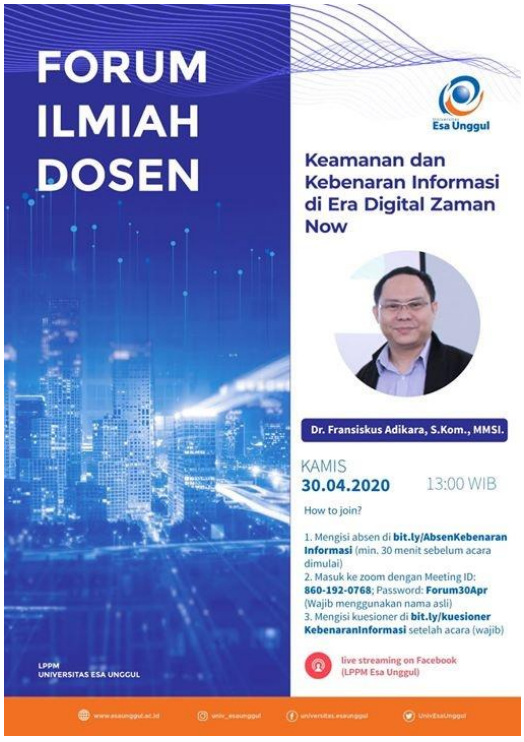
Pendahuluan

Keamanan Informasi di era Digital "Zaman *Now*" sangat erat hubungannya dengan keamanan penggunaan perangkat keras (*hardware*) maupun perangkat lunak (*software*) yang sangat erat hubungannya dengan kemajuan jaringan telekomunikasi khususnya internet(Ikenwe et al., 2016). Istilah-istilah yang muncul di era digital terkait keamanan informasi diantaranyakeamanan perangkat telekomu-nikasi, keamanan komputer, keamanan jaringan, keamanan dunia *cyber* (internet), proteksi data, keamanan pengguna teknologi dan lainnya(Rao & Nayak, 2014).

Masyarakat awam perlu memahami mengenai keamanan informasi karena saat ini dunia dan era digital mau tidak mau harus diterima oleh masyarakat umum, terlebih pada saat ini kita sedang dalam kondisi *Physical Distancing*. Penggunaan dan pemanfaatan teknologi informasi dan komunikasi semakin dibutuhkan dalam melaksanakan kegiatan bekerja, sekolah, maupun beribadah. Transaksi elektronik atau digital menjadi bagian dalam gaya hidup sehari-hari. Konsep mengenai keamanan dan kebenaran informasi digital saat ini harus dipahami dan dimengerti oleh masyarakat umum dan awam agar gaya hidup digital yang baru diadaptasi ini tidak

menjadi tantangan baru apalagi menjadi ancaman baru dalam berkomunikasi serta bertransaksi.

Kegiatan pengabdian kepada masyarakat sendiri merupakan kegiatan yang berperan untuk memberikan wawasan baru untuk masyarakat dari dunia pendidikan.Dengan adanya kegiatan pengabdian kepada masyarkat, peran perguruan tinggi akan membantu memberikan informasi dan pemahaman terbaru terhadap kemajuan ilmu pengetahuan maupun teknologi yang sedang berkembang dimasyarakat. Terutama saat ini bangsa Indonesia tidak terhindarkan dari kondisi pandemik Covid-19. Masyarakat umumnya menghadapi masa-masa baru yang lebih mengandalkan informasi dan transaksi digital. Masih banyak komponen masyrakat yang belum memahami mengenai informasi digital, khususnya dalam hal keamanan dan kebenarannya.Khususnya bagi para dosen dan tenaga pendidik yang saat ini harus menjalankan kegiatan perkuliahan secara jarak jauh. Konsep mengenai keamanan dan kebenaran digital harus dipahami oleh para pelaku pendidikan agar dalam menyampaikan informasi dapat berjalan dengan lancar serta tidak membahayakan bagi siapapun penggunanya.



Gambar 1
Media Informasi Kegiatan Forum Ilmiah Dosen Keamanan dan Kebenaran Informasi di Era Digital Zaman *Now*

Kegiatan ini diumumkan secara online melalui media sosial, pengirim pesan dan surat elektronik kepada para dosen, tenaga pendidik serta masyarakat umum yang hendak mengikuti kegiatan ini melalui media sosial (*live streaming*) (Gambar 1). Sesudah acara, video rekaman juga akan diunggah ke Youtube, pada channel Universitas Esa Unggul, sehingga bisa ditonton kapan saja oleh siapa saja yang mempunyai link tersebut.Dengan cara ini diharapkan semakin banyak peserta yang memerlukan pengetahuan akan keamanan dan kebenaran informasi digital dapat mengikuti kegiatan pengabdian kepada masyarakat.

Berbasis pada kajian di atas, maka kegiatan penyuluhan keamanan dan kebenaran informasi digital saat pandemik Covid-19 ini bertujuan agar para peserta dapat memahami konsep terkait keamanan informasi digital yang harus dijaga dan diperhatikan selama bekerja dari rumah di kondisi pandemik Covid-19. Selain itu juga peserta diharapkan dapat membedakan informasi digital yang benar dan salah, serta bijak dalam menyampaikan atau meneruskan informasi digital yang diperoleh dari pihak manapun.

Manfaat yang hendak dicapai dari kegiatanadalah agar keamanan informasi digital para peserta dapat semakin terjaga, baik yang berhubungunan dengan informasi pribadi, keuangan, maupun kesehatan. Selain keamanan informasi, penyebaran berita bohong atau hoaks (terkait kebenaran informasi) juga dapat semakin ditekan. Kesadaran dan kemampuan peserta untuk memilah informasi yang benar atau tidak diharapkan meningkat sehingga hoaks tidak menjadi bagian hidup masyarakat di masa pandemik Covid-19 ini.

Metode Pelaksanaan

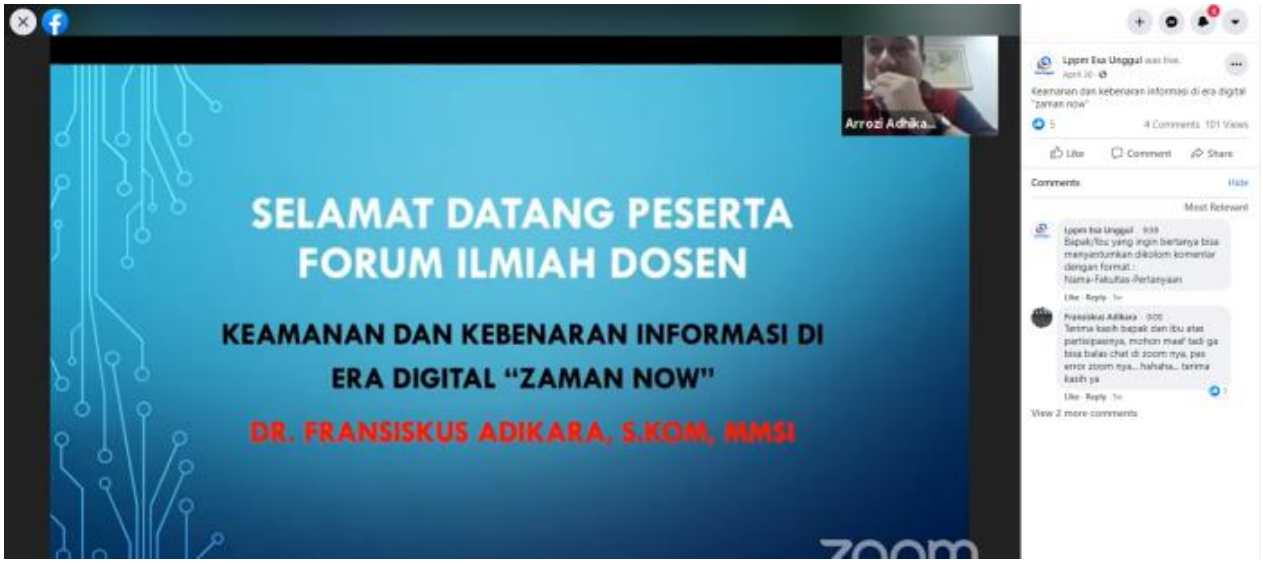
Di masa pandemik Covid-19 seperti sekarang ini, kegiatan-kegiatan penyuluhan dilakukan menggunakan media daring. Sebelum acara dimulai, kegiatan pengabdian kepada masyarakat ini diinformasikan ke para dosen serta tenaga pendidik menggunakan surat elektronik, pesan di whatsapp pada grup-grup komunitas, serta di sosial media Facebook. Kegiatan sudah dipersiapkan sejak dua minggu sebelum pelaksanaan, persiapan yang dilakukan adalah penyiapan materi yang akan disampaikan, rancangan *press release* yang akan dipublikasikan di media massa, serta kuesioner untuk melihat hasil dari kegiatan ini.

Pelaksanaannya dilakukan menggunakan perang-kat lunak Zoom untuk *webinar* dan *live streaming* pada media sosial Facebook. Tata cara yang dilakukan pada pelaksana acara adalah sebagai berikut :

1. Mengisi daftar kehadiran (absen) melalui bit.ly/AbsenKebenaranInformasi 30 menit sebelum acara dimulai
2. Wajib menggunakan nama asli pada username Zoom

3. Log in (masuk) ke aplikasi Zoom dengan menggunakan Meeting ID: 860-192-0768 dan password: Forum30Apr
4. Kegiatan ini juga disiarkan live melalui facebook.com/lppm.esaunggul
5. Mengisi kuesioner melalui bit.ly/kuesionerKebenaranInformasi setelah acara (wajib). E-Sertifikat hanya dibagikan bagi Bapak/ Ibu yang telah mengisi kuesioner.

Lokasi streaming dilakukan dari rumah pembicara dan panitia masing-masing pada hari Kamis tanggal 30 April 2020 pada jam 13.00 – 15.00, absensi dimulai 30 menit sebelum acara, panitia dan pembicara masuk ke perangkat lunak Zoom 15 menit sebelum acara dimulai, dan pengisian kuesioner dilakukan setelah acaraselesai sampai batas waktu jam 18.00 hari yang sama. Sesudah itu sertifikat diberikan kepada peserta maksimal 3x24 jam setelah pengisian kuesioner selesai.



Gambar 2
Live Streaming Via Sosial Media Facebook dan Perangkat Lunak Zoom

Para peserta diberikan materi mengenai hal-hal berikut ini:

1. Konsep dan teori keamanan Informasi.
2. Istilah-istilah umum pada ilmu keamanan informasi.
3. Pemahaman mengenai undang-undang terkait keamanan dan penyebaran informasi.
4. Pemahaman mengenai hoaks (berita bohong).
5. Konsep saring sebelum *sharing*.
6. Melakukan proses Tanya – Jawab terkait permasalahan keamanan dan kebenaran informasi digital.
7. Peserta mendapatkan materi terkait yang dipresentasikan.
8. Peserta mengisi kuesioner untuk mengevaluasi hasil penyuluhan.

Hasil dan Pembahasan

Penyuluhan Keamanan dan Kebenaran Informasi Digital di Masa Pandemik Covid-19

Untuk memperoleh pemahamanan mengenai keamanan informasi, maka pengertian awal dimulai dari arti keamanan yaitu "kondisi yang terbebas dari bahaya". Jadi, keamanan informasi (*Information Security* / *Infosec*) dapat diartikan sebagai suatu cara untuk mengkondisikan sebuah informasi agar tidak diakses, dirubah, disebarkan, dan atau dihapus oleh seseorang/sesuatu yang tidak berhak terhadap informasi tersebut". Untuk mendapatkan kemanan informasi ini, biasaya pengamanannya pun dijaga secara berlapis sebagai berikut : lapisan keamanan fisik, lapisan keamanan pribadi, lapisan keamanan operasional, lapisan keamanan komunikasi dan lapisan keamanan jaringan.

Untuk lebih jelasnya, kita pahami dulu 3 pilar keamanan informasi yaitu :

1. *Integrity*/Integritas : perlindungan terha-dap modifikasi yang tidak seharusnya atau perusakan informasi
2. *Availability*/Keberadaan : kepastian akan akses informasi untuk pengguna yang berwenang pada waktu dan kondisi yang diharapkan
3. *Confidentiality*/Kerahasiaan : jaminan bahwa informasi tidak diungkapkan kepada orang yang tidak berwenang

Gambar 3
Tiga Pilar Keamanan Informasi

Pada era digital dan bergantungnya masyarakat pada teknologi untuk membagikan informasi, maka berikut adalah hal-hal yang menyebabkan informasi perlu dilindungi, yaitu :

- Jaringan komputer dan internet sudah menjadi hal yang umum
- Internet sudah menjadi kebutuhan dasar dalam bekerja dan kehidupan
- Masih kurangnya kesadaran akan perlindungan informasi sehubungan dengan teknologi yang digunakan sehari – hari (prioritas rendah) contoh :
    - "Layanan jalan dulu, aman belakangan"
    - "Sejauh ini bisnis aman-aman saja dengan pengamanan seadanya"
    - "Perlu investasi dan waktu untuk keamanan informasi digital (MAHAL)"
    - "Sharing Password di sesama pengguna"

Isu-isu terkait dengan topik keamanan informasi di Era Digital "Zaman Now" ini terutama saat terjadinya pembatasan sosial berskala besar karena adanya pandemik COVID-19 yaitu :

- Pengetahuan mengenai Standard Kepatuhan di Keamanan Informasi khususnya berhubungan dengan informasi-informasi sensitive
- Penyebaran Informasi yang tidak tepat (hoaks)
- Keamanan Informasi pada Software yang digunakan saat WFH

Terkait standad kepatuhan (*Compliance Standard*) dari keamanan informasi, regulator telah menciptakan seperangkat peraturan, standar, dan kerangka kerja yang semakin besar yang bertujuan untuk menegakkan perlindungan informasi, privasi, dan transparansi informasi.Contoh standar kepatuhan yang dikeluarkan lembaga-lembaga di dunia dan berlaku umum yaitu :

- GLBA (*Gramm Leach Bliley Act*) untuk Pelayanan Finansial / Keuangan
- HIPAA (*Health Insurance Potability and Accountability Act*) untuk pelayanan kesehatan
- Sarbanes-Oxley untuk perusahaan publik
- PCI DSS (*Payment Card Industry Data Security Standard* (Standar Keamanan Data Industri Kartu Pembayaran)) untuk pemegang kartu kredit / bank
- COBIT (*Control Objective for Information and Related Technology*) untuk tata Kelola Teknologi Informasi
- NIST, ISO 27001, BSI Standard, FISMA, FERPA, dan lainnya

Contoh penerapan standar berdasarkan *Gramm Leach Bliley Act* (GLBA) yang berhubungan dengan pelayanan finansial/keuangan yaitu Undang-undang seharusnya mensyaratkan lembaga keuangan untuk melindungi informasi yang dikumpulkan tentang individu seperti:
Nama

- Alamat dan nomor telepon
- Rekening bank dan kartu kredit
- Nomor Jaminan Sosial
- Penghasilan dan sejarah kredit

Untuk sektor keuangan di Indonesia, keamanan informasi untuk perlindungan konsumen sektor jasa keuangan pada Peraturan Otoritas Jasa keuangan nomor : 1/POJK.07/2013. Dengan adanya aturan ini maka jika ada orang/individu yang tidak kita kenal seperti sales marketing yang menawarkan kartu kredit/asuransi/pinjaman/pelayanan keuangan lainnya dan tahu mengenai kondisi keuangan kita, maka kita berhak untuk menegur karena ada pelanggaran kemanan informasi di kasus ini. Seseorang juga seharusnya tidak membagikan informasi terkait transaksi keuangan orang lain yang tidak diketahui oleh orang tersebut.

Penerapan standar dari *Health Insurance Potability and Accountability Act* (HIPAA) yang berhubungan dengan pelayanan kesehatan mempunyai tujuan untuk :

- Menjamin perlindungan asuransi kesehatan karyawan
- Mengurangi penipuan dan penyalahgunaan perawatan kesehatan
- Lindungi informasi kesehatan individu dari akses tanpa persetujuan atau otorisasi

Yang dilindungi oleh HIPAA :

- Informasi Identifikasi Pribadi (*Personal Indentification Information*)

  - Pengidentifikasi langsung: nama individu, nomor BPJS, nomor SIM
  - Pengidentifikasi tidak langsung: informasi tentang seorang individu yang dapat dicocokkan dengan informasi lain yang tersedia untuk mengidentifikasi individu tersebut
- Informasi Kesehatan yang Terlindungi (*Personal Health Information*) yaitu Informasi Kesehatan yang Dapat Diidentifikasi secara Individual (*Individual Identification of Health Information*)

Dokumen-dokumen yang dilindungi dibuat atau diterima oleh penyedia layanan kesehatan, perencana kesehatan, atau rumah sakit.Dokumen tersebut berkaitan dengan masa lalu, kondisi kesehatan fisik atau mental masa depan atau kondisi seseorang (termasuk informasi terkait pembayaran untuk perawatan kesehatan). Dokumen yang dilindungi semua yang ditransmisikan dalam bentuk atau media apa pun — komunikasi kertas, elektronik, dan verbal.

Contoh Informasi Kesehatan yang Terlindungi :

- *Medical charts*
- *Problem logs*
- *Photographs and videotapes*
- *Communications between health care professionals*
- *Billing records*
- *Health plan claims records*
- *Health insurance policy number*

Terkait standar diatas, maka perlu kehati-hatian para masyarakat untuk tidak boleh sembarangan membagikan informasi terkait kesehatan seseorang apalagi tanpa sepengetahuan orang yang bersangkutan.

Selain masalah keamanan informasi, saat ini juga kita mengalami tantangan terhadap hoaks. Hoaks berdasarkan pengertian dari KBBI adalah informasi bohong. Selain itu secara umum, hoaks bisa diartikan juga sebagai informasi palsu, berita bohong, atau fakta yang diplintir atau direkayasa untuk tujuan lelucon hingga serius (politis). Yang termasuk juga dalam kategori hoaks adalah berita buatan atau berita palsu (*Fabricated News/Fake News*).

Terkait hoaks ini, banyak yang bisa kita pelajari dari sumber-sumber yang sudah mengeluarkan publikasinya, salah satunya dengan topik Saring sebelum Sharing, karena informasi saat ini terus meningkat penyebarannya terutama melalui internet, website, email, dan perangkat media sosial yang beragam. Kominfo sebagai lembaga negara sudah mengeluarkan juga ciri-ciri berita hoaks yang seharusnya mudah dipahami oleh masyarakat, karena saat ini menurut Pak Garuda dalam salah satu acara webminar Wantiknas menginformasikan bahwa di masa PSBB ini, Indonesia dalam kondisi darurat Hoaks yang terjadi dimana-mana.

Hasil dari Penyuluhan Revolusi Industri 4.0 di Dunia Pendidikan

Setelah penyuluhan berjalan, maka proses berikutnya menerima tanggapan dan pertanyaan dari para peserta.Sesudah pertanyaan selesai maka berikatnya para peserta mengisi kuesioner. Pertanyaaan pertama : Bagaimana menilai sebuah informasi itu benar atau hoaks ? Jawabannya bisa menggunakan patokan ciri-ciri hoaks yang dikeluarkan Kominfo, yaitu :

1. Sumber informasi dan medianya tidak jelas identitasnya, mengeksploitasi fanatisme SARA .
2. Pesan tidak mengandung unsur 5W+1H lengkap.
3. Pihak yang menyebarkan informasi meminta info tersebut disebarluaskan semasif mungkin.
4. Hoaks diproduksi untuk menyasar kalangan tertentu.

Selain itu juga bisa memanfaatkan situs-situs pencarian informasi atau website cekfakta.com yang berguna sebagai konfirmasi berita yang ada.

Pertanyaan kedua situs belanja online yang meminta foto kartu identitas penggunanya ? Jawaban dari pertanyaan ini kalau untuk berbelanja seharusnya tidak perlu sampai meminta kartu identitas pembeli, biasaanya yang diminta jika pengguna mau melakukan transaksi penjualan, gunanya adalah menjadi jaminan untuk pembeli agar barang yang dijual sesuai dengan apa yang dipasarkan.

Pertanyaan ketiga yaitu terkait dengan aplikasi Zoom yang dikatakan kurang aman untuk digunakan ? Jawabannya aplikasi Zoom sendiri terus melakukan perbaikan terhadap kebocoran maupun celah-celah keamanan yang dimilikinya, seperti hal aplikasi yang lainnya, ketika pengguna masih sedikit dan tidak banyak, pasti faktor keamanan belum menjadi faktor utama dalam membuat fungsi, namun sejalan dengan penggunaannya yang semakin banyak, maka keamanan sistem pasti akan terus selalu ditingkatkan.

Pertanyaan terakhir yaitu bagaimana mengamankan akun aplikasi pesan seperti whatsapp yang sering terjadi pencurian identitas ?Jawabannya yaitu dengan menerapkan dua langkah verifikasi untuk akun tersebut. Walaupun akan menjadi lebih kurang nyaman dalam penggunaannya karena harus melakukan dua langkah pengamanan, hal ini lebih menjamin sistem tidak mudah untuk dicuri.

Kesimpulan

Dari kegiatan ini dapat disimpulkan bahwa para peserta 99% menyadari bahwasanya keamanan

informasi sangat penting untuk dipelajari dan dipahami khususnya dimasa pandemik Covid-19 yang mengharuskan semua mengandalkan teknologi informasi dan komunikasi dalam melaksanakan kehidupan sehari-hari. Para peserta juga sudah 95% memahami terkait keamanan informasi, baik yang berhubungan dengan informasi keuangan maupun informasi pribadi terkait kesehatan seseorang.

Selanjutnya perlu dilaksanakan kegiatan peng-abdian pada masyarakat yang berkelanjutan di bidang teknologi informasi dan komunikasi terkait tentang antisipasi selanjutnya setelah masa Covid-19 ini berakhir. Penggunaan teknologi informasi dan komuikasi bagaimanapun akan terus berkembang penggunaannya.

Daftar Pustaka

Ikenwe, I. J., Igbinovia, O. M., & Elogie, A. A. (2016). Information Security in the Digital Age: The Case of Developing Countries. *Chinese Librarianship: An International Electronic Journal*, *42*(December 2017). http://www.iclc.us/cliej/cl42IIE.pdf

Rao, U. H., & Nayak, U. (2014). *The InfoSec Handbook*. Apress. https://doi.org/10.1007/978-1-4302-6383-8