Journal Of Dedicator Community
ISSN: 2548-8783 (p); 2548-8791 (e), Vol 7 No 1 April 2023: 079 - 094
DOI: https://doi.org/10.34001/jdc.v6i2.3775

Peningkatan Literasi Digital Mahasiswa UNUSA Untuk Pengamanan Data Pribadi

Rizqi Putri Nourma Budiarti[1], Dike Bayu Magfira[2], Nur Shabrina Meutia[3], Afib Rulyansah[4]
[1,2,3]Department of Information Systems, Universitas Nahdlatul Ulama Surabaya, Surabaya [4]Department of Elementary School Teacher Education, Universitas Nahdlatul Ulama Surabaya, Surabaya.

Key word:

Digital Literacy; Social Media; Data Security; Digital Applications; Digital Education.

Abstract

The transformation of the digital 4.0 era and the use of social media by millennials provides easy disclosure of personal data. This is caused by several applications downloaded by millennials, who sometimes ignore the agreement rules at the start of the installation of each application which are often provided in English and often ignore previous user judgments. Even from the advertisements that are spread, not a few install applications and are trapped in online loans by submitting personal data and other personal information in accessing data on their cellphones. Lack of knowledge related to digital literacy in securing personal data can lead to inappropriate use of personal data. There is learning such as an introduction to internet ethics, an introduction to basic ethical hacking related to the introduction of protocols and spoofing and the sharing of information about the security of information assets is urgently needed. the importance of protecting personal data so that it is not misused by irresponsible people. Therefore, learning internet ethics and basic introduction to ethical hacking for data security can be a solution in an open digital era.

Kata Kunci

Literasi Digital; Media Sosial; Keamanan Data; Aplikasi Digital; Edukasi Digital.

Abstrak

Transformasi era digital 4.0 dan penggunaan media sosial oleh para milenial memberikan keterbukaan data personal secara mudah. Hal ini disebabkan oleh beberapa aplikasi yang didownload oleh para milenial, dimana kadang tidak menghiraukan aturan kesepakatan dalam permulaan instalasi setiap aplikasi yang sering disediakan dalam bahasa inggris dan seringkali tidak menghiraukan penilaian user sebelumnya. Bahkan dari iklan yang tersebar, tidak sedikit yang menginstall aplikasi dan terjebak dalam pinjaman online dengan menyerahkan data pribadi dan informasi personal lainnya dalam mengakses data didalam handphonenya. Kurangnya pengetahuan terkait literasi digital dalam pengamanan data pribadi sehingga dapat menyebabkan penggunaan data pribadi yang tidak sesuai harapan. Adanya pembelajaran seperti pengenalan etika berinternet, pengenalan dasar ethical hacking terkait pengenalan protocol dan spoofing serta pembagian informasi seputar keamanan aset informasi sangat dibutuhkan.Melalui pengabdian masyarakat berbasis pembelajaran digitalisasi ini, edukasi digital terkait peningkatan literasi digital keamanan data pribadi yang dikhususkan bagi Mahasiswa UNUSA agar memahami pentingnya menjaga data pribadi agar tidak disalahgunakan oleh orang-orang yang tidak bertanggung jawab. Oleh karena itu, pembelajaran etika berinternet serta pengenalan dasar ethical hacking untuk pengamanan data bisa menjadi solusi di era digital yang serba terbuka.

PENDAHULUAN

Perkembangan teknologi yang semakin pesat telah menyediakan ruang terbuka bagi tersedianya software-software yang justru semakin meningkat dan memberikan kemudahan untuk bisa mengakses data dimanapun dan kapan pun. Namun kadang tidak diimbangi dengan fitur untuk keamanan datanya bahkan kadang-kadang yang terjadi di kalangan programmer saat membuat suatu aplikasi dan tidak terlalu memprioritaskan dari sisi keamanannya (Veracode, 2020), (HBR Staff, 2018), (Synopsys, 2020), (Sotnikov, I, 2019). Hal ini merujuk dari beberapa artikel diantaranya Khan, M. A., & Khan, S. U. menjelaskan bahwa keamanan dari berbagai teknik keamanan perangkat lunak seperti enkripsi, obfuskasi, sanitasi input dan pemodelan keamanan bisa menjadi pertimbangan kemungkinan serangan keamanan dan penulis menunjukan pentingnya melakukan pengujian keamanan dan manajemen resiko dalam keamanan software dimana dapat pula dilakukan pemahaman yang lebih baik tentang berbagai teknik keamanan perangkat lunak yang dapat digunakan untuk meningkatkan keamanan perangkat lunak (Khan, M. A., & Khan, S. U., 2019). Artikel yang ditulis oleh Huang, dkk membahas tentang pengujian keamanan perangkat lunak dan teknik pengujian seperti fuzz testing dan pengujian penetrasi. Penulis menunjukkan kelemahan dari teknik pengujian keamanan yang digunakan saat ini dan menyarankan peningkatan pengujian keamanan secara menyeluruh sehingga dapat mengidentifikasi celah keamanan dan memperkuat keamanan perangkat lunak (Huang, X., Xu, W., Liu, Y., Wang, J., & He, Q. , 2021). Ketika membangun sebuah aplikasi yang memiliki user interface dan user experience yang sangat menarik kadang hanya memikirkan cara melakukan pengetesan sistemnya saja tanpa menitikberatkan pada keamanan data yang melekat pada software yang tersedia dan direlease di ruang publik dengan keamanan yang semakin baik. Kadang masalah timbul dikarenakan cukup banyak kelemahan yang ditemukan didalam aplikasi sistem informasi dan proses penangannya kurang cepat dimana sering ditemukan keamanan jaringannya sangat rentan diretas, dan ketika dilakukan filter port pada sistemnya ternyata banyak port yang seharusnya tertutup menjadi terbuka dan tidak sesuai fungsinya, bahkan kadang tidak dilakukannya maintenance berkala terhadap penggunaan software ataupun akses jaringannya. Salah satunya, teknologi informasi yang sering digunakan di kalangan kaum milenial seperti mahasiswa adalah aplikasi berbasis website dan aplikasi berbasis mobile phone misalkan

aplikasi game, dimana ancaman terkait keamanan data mereka sangatlah tinggi. Hal ini memudahkan data mereka diakses dan dipergunakan oleh orang-orang yang tidak bertanggung jawab, terutama bagi para millennial yang jarang sekali membaca manual kontrak saat proses penginstalan aplikasi karena sering kali tersedia dalam bahasa yang bukan menggunakan bahasa Indonesia sehingga aplikasi tersebut secara tidak langsung bisa mengakses data mereka dengan mudah. Kondisi ini juga akibat semakin banyak tersedianya berbagai software yang dapat digunakan dalam melakukan hacking sehingga memudahkan mahasiswa untuk belajar secara otodidak bagaimana membobol suatu sistem, Namun bila tidak diimbangi oleh meningkatnya pengetahuan terkait etika dalam melakukan pembobolan sistem, sehingga seringkali etika dalam melakukan hacking tidak dilakukan dan yang tidak diharapkan adalah hal ini menjadi salah satu penyebab meningkatnya kriminalitas dari aksi pembobolan sistem dibeberapa tahun terakhir ini.

Maraknya mahasiswa yang terjebak dalam pinjaman online tanpa mahasiswa tersebut menyadari proses pendaftarannya ke aplikasi dan melakukan pinjaman online, yang kadang menyebabkan mereka menyerahkan data pribadi dan informasi personal lainnya sehingga aplikasi tersebut mudah dalam mengakses data didalam handphonenya. Proses peretasan pun bisa dilakukan di media sosial para milenial, sehingga tidak jarang terjadi tiba-tiba akses twitter, instagram bahkan facebook mereka berpindah tangan dan akses sehingga membuktikan otentifikasi bisa dilakukan oleh yang bukan pemiliknya, karena data personal seperti password pada aplikasi tersebut sudah diketahui oleh orang lain. Peretas atau yang sering dikenal dengan istilah hacker atau craker adalah orang yang mempelajari dan melakukan analisis serta memodifikasi suatu aplikasi agar dapat menerobos masuk ke dalam suatu sistem yang terhubung melalui jaringan internet di ruang public namun memiliki fungsi yang berbeda. Peretas hacker yang disebut sebagai *white hat hacker* biasanya memikirkan aksi yang dilakukan, dimana ketika menerobos suatu sistem, mereka bisa memperbaiki sistem tersebut. Hal ini berbeda, dengan *black hat hacker* Ketika melakukan penerobosan sistem dilakukan dengan tujuan tertentu seperti untuk uang dan keperluan lainnya seperti menghancurkan data pada sistem tersebut tanpa seizin pemiliknya.Berbeda dengan halnya cracker, dimana penerobosan sistem yang dilakukan biasanya hanya sekedar untuk main-main saja, dan biasanya mereka terampil tetapi ceroboh

sehingga mudah diketahui identitasnya tetapi mereka memahami bahasa pemrograman pada sistem dengan baik, namun peretasannya biasanya juga tanpa izin dari pemiliknya.

Etika didalam berinternet dan etika ketika melakukan penerobosan sistem perlu dikenalkan kepada kaum milenial terutama mahasiswa yang berada dilingkungan sistem informasi dan berkecimpung di dunia TIK (Teknologi Informasi dan Komputer) yang biasanya mereka sering membuat aplikasi dalam berbagai penggunaan sistem informasi seperti aplikasi e-business (Garbowski et al., 2019), e-wakaf (Sukron et al., 2020), e-commerse (Subchan & Setiadi, 2020), e-education (Budiarti & Pratomo, 2018; Salim et al., 2020), e-IoT (Budiarti et al., 2018, 2019; Yohanie et al., 2018), e-government (Bandiyono & Indrianto, 2019; Rahayuda, 2017), bahkan aplikasi layanan lainnya yang seringkali mereka melakukan developing mandiri tanpa memperhatikan keamanan data dari tiap aplikasinya ataupun memperhatikan etika didalam sistemnya padahal masalah dalam etika ini perlu mendapatkan perhatian khusus dalam penggunaan sistem informasi yang terhubung dengan internet. Etika dalam penggunaan suatu aplikasi pada sistem informasi biasanya berkaitan dengan perihal keamanan data pribadi, dan penggunaan hak akses. Ethical Hacking merupakan suatu aktifitas yang berkaitan dengan etika dalam melakukan peretasan ke dalam aplikasi dengan melakukan izin terkait aktifitas ini, sehingga mendapatkan hak akses atas data dan sistem dari suatu organisasi yang tertuang dalam sebuah kontrak dan biasanya tujuannya adalah untuk menguji keamanan jaringan mereka. Kemampuan dasar yang dimiliki biasanya dapat melakukan scanning terhadap sistem informasi yang ada untuk mengetahui apakah sistem informasi tersebut memiliki kelemahan dan hasilnya berupa laporan keamanan terhadap sistem informasi tersebut. Terdapat beberapa metode peretasan didalam ethical hacking diantaranya, *reconnaissance* (pengintaian) (Patil et al., 2017), *scanning* (pemindai) (Smith et al., 2002), *gaining access* (mendapatkan akses) (Munjal, 2014), *maintaining access* (mempertahankan akses) (Harper et al., 2022), *clearing tracks* (menghapuskan jejak) (Ushmani, 2018).

Hal yang berkaitan dengan keamanan data pribadi sebenarnya sudah diatur aturannya melalui Peraturan Menteri No 20 Tahun 2016 tentang Perlindungan Data Pribadi (PDP) ditetapkan 7 November 2016, diundangkan dan berlaku sejak 1 Desember 2016. Dari dokumen yang diunduh, di aturan itu dinyatakan bahwa data pribadi adalah data perseorangan tertentu yang disimpan, dirawat, dan dijaga kebenaran

serta dilindungi kerahasiaannya. Selain itu, berkaitan dengan aturan undang-undang terkait adanya peretasan data yang dikategorikan sebagai Tindakan criminal menggunakan teknologi cyber yang diatur dalam undang-undang nomor 36 tahun 1999 (Hermawan, 2015) terkait kejahatan dan pelanggaran computer dan cyber serta sanksi administrasinya serta diatur juga melalui undang-undang no 11 tahun 2008 tentang informasi dan transaksi elektronik (UU ITE) (Putra & Widiatedja, 2015) dan perumusan pidananya diatur didalamnya (Sartika et al., 2020).

Berdasarkan data yang diperoleh tim pengabdian masyarakat melakukan wawancara dan observasi yang telah dilakukan terhadap mahasiswa peserta pelatihan diperoleh bahwa, tidak jarang bagi mereka ketika membangun suatu aplikasi sistem informasi merasa bahwa kurang penting bagi keamanan data itu dipasang pada aplikasi mereka dengan alasan aplikasi yang mereka buat dan direlease diruang publik adalah free, tanpa membebankan biaya tertentu kepada penggunanya. Sehingga, keamanan aplikasi sistem informasi yang dibuat hanya untuk mempermudah pekerjaan di dunia IT, dan keamanan datanya merupakan prioritas terakhir saja atau tetap merupakan tanggung jawab pribadi bagi para penggunanya. Dengan permasalahan diatas sehingga diperlukan peningkatan literasi digital bagi para mahasiswa yang berkecimpung di dunia IT terutama di bidang teknologi bahwa dosen harus berperan aktif dalam membantu peningkatan literasi digital melalui pemberian pelatihan dan sosialisasi terkait keamanan data pribadi dan etikanya terutama kepada kaum milenial khususnya dalam hal ini mahasiswa UNUSA agar lebih memperhatikan keamanan data pribadinya dan lebih *aware* dalam melakukan *developing* sistem informasi yang dibuatnya dengan tetap memperhatikan etika dalam keamanannya melalui ethical hacking. Di tinjau dari faktor kebermanfaatannya, dengan adanya pelatihan ini secara tidak langsung dapat membantu meningkatkan keamanan data pribadi mahasiswa UNUSA khususnya di prodi Sistem Informasi menjadi lebih baik, dimana mahasiswa yang memiliki keahlian IT bisa mempelajari ilmu pemrograman tanpa keluar dari batasan-batasan etika. Apalagi situasi seperti pasca pandemi covid19 adaptasi menghadapi situasi pandemi yang merupakan salah cara dimana tingkat penggunaan internet *pasca* pandemic meningkat sehingga sudah menjadi kebiasaan bagi mahasiswa mengakses internet, untuk berselancar, pembelajaran *online*, dan bahkan mencari berbagai *software* untuk pendukung aktifitas pembelajaran praktikumnya yang kadang diperoleh dari pihak ketiga yang

diragukan keamanannya. Beberapa penelitian terdahulu terkait keamanan data pada aplikasi berbasis komputer dan pengetahuan terkait *ethical hacking* diantaranya terkait pengetahuan *ethical hacking*(Harper et al., 2022; Munjal, 2014; Patil et al., 2017; Smith et al., 2002), *wireshark*(Sandhya et al., 2017; Singh, 2019), *sniffing dan scanning*(Juneja, 2013; SRIDHAR, n.d.), undang-undang terkait peretasan data, penggunaan password untuk keamanan asset informasi seperti *two-verification authentification*((Han et al., 2003; Matyas & Riha, 2003), serta meng-*update password*-nya secara berkala((Habib et al., 2018; Kumar et al., 2016).

Berdasarkan permasalahan yang telah disebutkan di atas, maka upaya yang bisa dilakukan untuk meningkatkan keamanan data pribadi khususnya para mahasiswa di Universitas Nahdlatul Ulama Surabaya dalam meningkatkan literasi digital terkait pengetahuan dan penggunaan aplikasi baik yang berbasis website ataupun android, maka diadakan pelatihan ethical hacking untuk keamanan data pribadi mahasiswa UNUSA. Program ini diharapkan dapat memberikan pengaruh yang positif dalam memenuhi kebutuhan keamanan data para mahasiswa agar lebih peduli terkait data pribadinya, tidak melakukan kegiatan yang melanggar etika dalam berinternet maupun dalam melakukan kegiatan peretasan. Diharapkan juga dari program ini, tim pengabdian masyarakat dapat mengetahui tingkat pemahaman peserta pelatihan literasi digital berbasis keamanan data pribadi di Universitas Nahdlatul Ulama Surabaya. Adapun solusi-solusi lainnya yang diharapkan pada kegiatan pengabdian masyarakat ini diantaranya, pengenalan literasi digital terkait etika berinternet, adanya penambahan pengetahuan terkait literasi digital tentang pentingnya penggunaan ethical hacking, pemberian informasi terkait undang-undang keamanan data dan sosialisasi terkait software-software yang bisa digunakan untuk sniffing dan scanning sehingga mengantisipasi akses port yang terbuka dari aplikasi tertentu.

METODE

Dalam pelaksanaan pengabdian masyarakat ini, tim pengabdian masyarakat bekerja sama dengan mahasiswa-mahasiswa ukm cyber computer and security menggunakan metode pengabdian dalam bentuk sosialisasi berupa pemaparan edukasi digital terkait etika berinternet dalam penggunaan data digital dan pembelajaran kode etik terkait undang-undang digital dilanjutkan dengan pelatihan ethical hacking serta pemberian kuisioner sebelum kegiatan (pre-test) dan sesudah kegiatan (post-test). Dalam melaksanakan

kegiatan pengabdian masyarakat di Universitas Nahdlatul Ulama Surabaya dibagi menjadi tiga tahapan yaitu tahap persiapan, tahap pelaksanaan kegiatan, dan tahap evaluasi kegiatan.

2.1. Tahap Persiapan

Adapun pada tahap persiapan, beberapa hal yang dilakukan diantaranya, penyusunan kegiatan sosialisasi dan pengabdian masyarakat terkait literasi digital keamanan data personal, dilanjutkan dilakukan observasi menyeluruh melalui wawancara untuk mengetahui tingkat pengetahuan dan pemahaman mahasiswa UNUSA terkait etika berinternet, etika dalam pengamanan data termasuk ethical hacking pada sistem. Pada akhir tahapan persiapan ini, breakdown kerangka masalah terkait data dan materi apa saja yang dibutuhkan dan oleh tim pengabdian masyarakat dimana kerangka tersebut akan dipaparkan dalam sub-sub materi melalui diskusi saat survey lapangan dan pembagian kuisioner pre-test terkait pemahaman mahasiswa UNUSA terkait etika berinternet, etika dalam pengamanan data termasuk ethical hacking pada sistem.

2.2. Tahap Pelaksanaan Kegiatan

Adapun pada tahap pelaksanaan kegiatan, beberapa hal yang dilakukan diantaranya, menerapkan rencana kegiatan pengabdian masyarakat yang telah disusun terkait literasi digital pengamanan data pribadi kepada mahasiswa di Universitas Nahdlatul Ulama Surabaya, dilanjutkan sosialisasi terkait etika berinternet dan pentingnya pengamanan data pribadi, pemahaman terkait kebutuhan-kebutuhan yang perlu dipersiapkan seperti software apa saja yang perlu diinstall dan penggunaannya selama pelatihan dan pelatihan ethical hacking pada sistem hingga sosialisasi terkait pembelajaran kode etik dan undang-undang terkait pengamanan data digital yang dilakukan kepada mahasiswa di Universitas Nahdlatul Ulama Surabaya.

2.3. Tahap Evaluasi Kegiatan

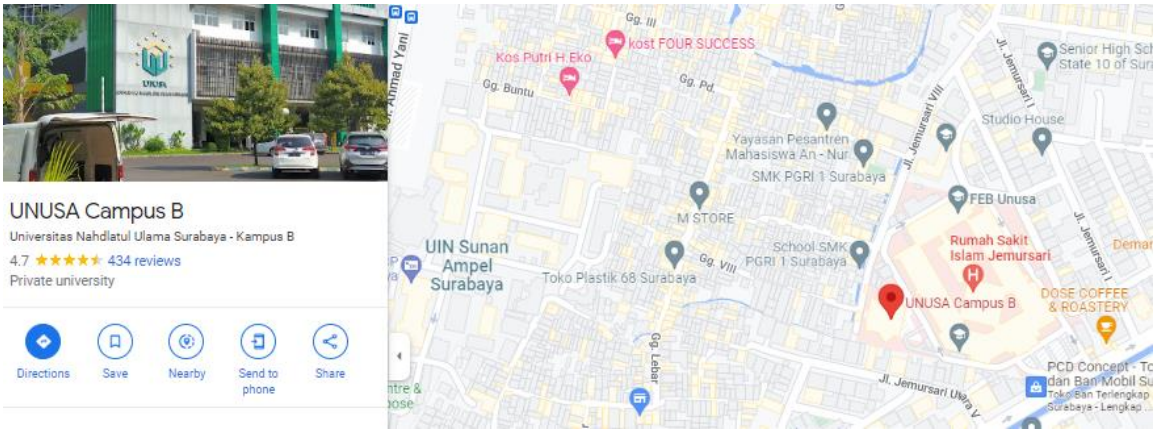
Adapun pada tahap evaluasi kegiatan, dilakukan untuk mengetahui hasil dari pelaksanaan pengabdian masyarakat ini, terkait pemahaman mahasiswa UNUSA terkait pemahaman literasi digital terhadap pengamanan data pribadi, dan pemaparan materi terkait etika dalam berinternet dan pengenalan ethical hacking melalui sosialisasi terkait materi ethical hacking, pendampingan installasi aplikasi seperti wireshark dan pendampingan selama praktek sniffing dan scanning sistem disamping saran penggunaan aplikasi yang berasal dari resources yang jelas dan menggunakan two-verification authentification atau meng-update password-nya secara berkala. Selain itu, dilakukan pembagian kuisioner post-test

untuk mengetahui apakah terjadi peningkatan pemahaman dari peserta mahasiswa di Universitas Nahdlatul Ulama Surabaya khususnya mahasiswa yang berasal dari prodi sistem informasi.

Gambar 1. Metode Pelaksanaan Pengabdian Masyarakat

HASIL

Kegiatan pengabdian masyarakat ini dilaksanakan di Universitas Nahdlatul Ulama Surabaya Kampus B, dimana memerlukan waktu pelaksanaan sekitar 3 minggu untuk kegiatan pelatihan dan sosialisasi terkait pengamanan data pribadi. Pada minggu pertama hingga minggu ke-tiga, dilakukan tahapan pre-test, tahapan kegiatan dan tahapan post-test dimana jumlah peserta yang mengikuti kegiatan pengabdian masyarakat ini adalah berjumlah 50 orang. Lokasi tempat pelatihan berada di Universitas Nahdlatul Ulama Surabaya Kampus B dapat dilihat pada Gambar 2.



Gambar 2. Lokasi Universitas Nahdlatul Ulama Surabaya

p-ISSN : 2548-8783
e-ISSN : 2548-8791

PEMBAHASAN

Berdasarkan data-data yang diperoleh dari pre-test terhadap pemahaman mahasiswa unusa, maka sosialisasi, pelatihan dan pendampingan yang dilakukan adalah sebagai berikut:

1. Menjelaskan terkait etika digital dalam berinternet.
2. Menjelaskan terkait pengenalan ethical hacking terkait pengenalan protocol dan spoofing.
3. Pelatihan dan praktek menggunakan wireshark, sniffing dan scanning.
4. Pendampingan terkait penggunaan two-verification authentification system dan update password berkala.

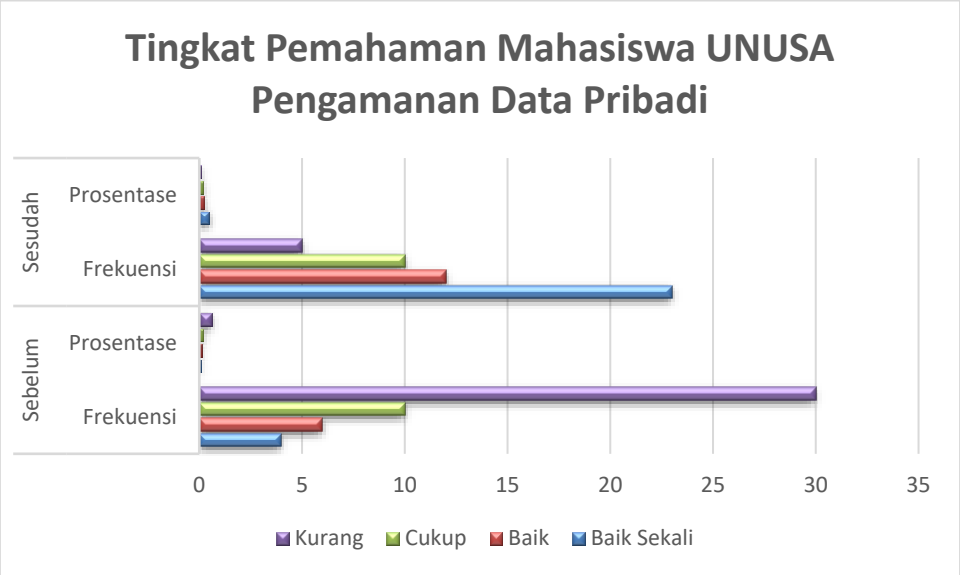
Pelaksanaan kegiatan ini, sangat menarik minat mahasiswa UNUSA karena dengan adanya pengabdian masyarakat ini bisa menambah pengetahuan dan literasi digital terkait pengamanan data sehingga membantu meningkatkan kemampuan mahasiswa unusa dalam menguji sistem informasi yang mereka bangun dan lebih memperdulikan keamanan digital terhadap penggunaan data pribadinya. Adapun hasil penilaian dan pengamatan tim pengabdian masyarakat, terkait pengukuran tingkat pemahaman peserta baik saat pretest penilaian sebelum kegiatan pengabdian masyarakat ini berlangsung dan posttest yang dilakukan setelah kegiatan telah dilaksanakan. Berikut hasil pengukuran tingkat pemahaman dapat dilihat pada Tabel 1.

Table 1. Pengukuran Tingkat Pemahaman Peserta Pelatihan Pengamanan Data Pribadi

Tingkat Pemahaman Keamanan Data Pribadi	***Pre-test***		***Post-test***	
	Frekuensi	Prosentase(%)	Frekuensi	Prosentase (%)
Baik Sekali	4	8%	23	46%
Baik	6	12%	12	24%
Cukup	10	20%	10	20%
Kurang	30	60%	5	10%
Jumlah	50	100%	50	100%

Hasil kegiatan pengabdian masyarakat terkait peningkatan literasi digital mahasiswa terkait pengamanan data pribadi menunjukan bahwa adanya peningkatan pemahaman dari peserta sekitar 38% pada kriteria baik sekali, 12% pada kriteria baik, tidak ada peningkatan 0% pada kriteria cukup dan pada kriteria kurang, mengalami penurunan sebanyak 50% dikarenakan peserta yang semula termasuk belum dapat memahami terkait literasi digital pada pengamanan data pribadi sudah menjadi

lebih paham setelah mengikuti kegiatan pengabdian masyarakat ini. Adapun solusi alternatif dan keberlanjutan pada kegiatan pengabdian masyarakat ini, diantaranya pemanfaatan literasi digital melalui sosialisasi pentingnya data pribadi, resiko kebocoran data dan etika digital dalam berinternet dengan dilakukannya pendampingan terkait workshop penggunaan aplikasi-aplikasi yang diperlukan pengamanan data pribadi, pendampingan dan pendekatan keilmuan melalui praktek pengamanan data pribadi dan beberapa software yang digunakan dalam praktek ethical hacking wireshark, kegiatan sniffing dan scanning yang didalamnya juga memberikan pemahaman terkait etika dalam peretasan data. Selain itu, pendekatan personal melalui komunitas sebagai wadah diskusi untuk melakukan evaluasi sistem dan pengecekan sistem secara berkala seperti menggunakan two-verification authentification atau meng-update password-nya secara berkala serta wadah bila menemukan kesulitan didalam penyelesaian terkait keamanan data pribadi. Berikut gambar grafik pemahaman peserta pelatihan pengamanan data pribadi dan pengenalan ethical hacking bagi mahasiswa UNUSA yang dapat dilihat pada Gambar 3 dan pelaksanaan kegiatan dapat dilihat pada Gambar 4.



Gambar 3. Grafik Tingkat Pemahaman Mahasiswa UNUSA Peserta Pelatihan

p-ISSN : 2548-8783
e-ISSN : 2548-8791

Gambar 4. Pelaksanaan kegiatan pengabdian masyarakat pengamanan data pribadi.

SIMPULAN DAN SARAN

Kegiatan pengabdian ini berhasil menarik minat peserta terhadap pembelajaran digital literasi website dan peningkatan terkait pemahaman terhadap pengamanan data pribadi. Selain itu, peserta pelatihan mendapatkan edukasi digital dan pendampingan yang baik yang dapat dilihat dari beberapa kali pelaksanaan pelatihan

dan pengenalan ethical hacking dalam kegiatan penggunaan aplikasi wireshark, kegiatan sniffing dan scanning serta pertanyaan yang diajukan peserta pelatihan kegiatan ini diharapkan dapat membantu mahasiswa UNUSA khususnya prodi sistem informasi dalam meningkatkan literasi digital terkait pengamanan data pribadi dan selalu melakukan update keamanan datanya menggunakan two-verification authentification atau meng-update password-nya secara berkala dan lebih berhati-hati dalam menggunakan software yang belum jelas.

DAFTAR PUSTAKA

Veracode. (2020). State of Software Security. https://www.veracode.com/state-of-software-security-report

HBR Staff. (2018). The Cybersecurity Risks Are Worse Than You Think. Harvard Business Review. https://hbr.org/2018/03/the-cybersecurity-risks-are-worse-than-you-think

Synopsys. (2020). Building Security in Maturity Model (BSIMM) 12. https://www.synopsys.com/content/dam/synopsys/sig-assets/reports/bsimm12-executive-summary.pdf

Sotnikov, I. (2019). Why Security Testing Is More Important Than Ever Before. Forbes. https://www.forbes.com/sites/forbestechcouncil/2019/06/19/why-security-testing-is-more-important-than-ever-before/Khan, M. A., & Khan, S. U. (2019). A review of software security techniques. Journal of Ambient Intelligence and Humanized Computing, 10(9), 3725-3741.

Huang, X., Xu, W., Liu, Y., Wang, J., & He, Q. (2021). A survey on security testing for software systems. Journal of Systems and Software, 178, 110948.

Bandiyono, A., & Indrianto, N. P. P. (2019). E-Rekon LK Application as a Form of Accounting and E-Government Information Systems Implementation in Indonesia. *International Journal of Innovation, Creativity and Change*, *8*(3), 23–40

Budiarti, R. P. N., Maulana, J., & Sukaridhoto, S. (2018). Aplikasi DIY Smart Trash Berbasis IoT Open Platform. *Applied Technology and Computing Science Journal*, *1*(2), 93–104.

Budiarti, R. P. N., & Pratomo, I. (2018). Pembuatan Sistem Informasi E-Book (Serbuk) Sebagai Media Pembelajaran Siswa Di SMA Negeri 1 Gresik. *Community Development Journal*, *2*(1).

Budiarti, R. P. N., Tjahjono, A., Hariadi, M., & Purnomo, M. H. (2019). Development of IoT for Automated Water Quality Monitoring System. *2019 International Conference on Computer Science, Information Technology, and Electrical Engineering (ICOMITEE)*, 211–216.

Garbowski, M., Drobyazko, S., Matveeva, V., Kyiashko, O., & Dmytrovska, V. (2019). Financial accounting of E-business enterprises. *Academy of Accounting and Financial Studies Journal*, *23*, 1–5.

Habib, H., Naeini, P. E., Devlin, S., Oates, M., Swoopes, C., Bauer, L., Christin, N., & Cranor, L. F. (2018). User behaviors and attitudes under password expiration policies. *Fourteenth Symposium on Usable Privacy and Security (SOUPS 2018)*, 13–30.

Han, C.-C., Cheng, H.-L., Lin, C.-L., & Fan, K.-C. (2003). Personal authentication using palm-print features. *Pattern Recognition*, *36*(2), 371–381.

Harper, A., Linn, R., Sims, S., Baucom, M., Fernandez, D., Tejeda, H., & Frost, M. (2022). *Gray hat hacking: the ethical hacker's handbook*. McGraw-Hill Education.

Hermawan, R. (2015). Kesiapan Aparatur Pemerintah dalam Menghadapi Cyber Crime di Indonesia. *Faktor Exacta*, *6*(1), 43–50.

Juneja, G. K. (2013). Ethical hacking: a technique to enhance information security. *International Journal of Innovative Research in Science, Engineering and Technology*, *2*(12), 7575–7580.

Kumar, R., Amin, R., Karati, A., & Biswas, G. P. (2016). Secure remote login scheme with password and smart card update facilities. *Proceedings of the 4th International Conference on Frontiers in Intelligent Computing: Theory and Applications (FICTA) 2015*, 495–505.

Matyas, V., & Riha, Z. (2003). Toward reliable user authentication through biometrics. *IEEE Security \& Privacy*, *1*(3), 45–49.

Munjal, M. N. (2014). Ethical hacking: an impact on society. *Cyber Times Int J Technol Manag*, *7*, 922–931.

Patil, S., Jangra, A., Bhale, M., Raina, A., & Kulkarni, P. (2017). Ethical hacking: The need for cyber security. *2017 IEEE International Conference on Power, Control, Signals and Instrumentation Engineering (ICPCSI)*, 1602–1606.

Putra, R. C. W., & Widiatedja, I. G. N. P. (2015). PERLINDUNGAN HUKUM BAGI KORBAN PENCURIAN

INFORMASI PRIBADI MELALUI DUNIA CYBER DITINJAU DARI UNDANG-UNDANG NO. 11 TAHUN 2008 TENTANG INFORMASI DAN TRANSAKSI ELEKTRONIK (UU ITE). *Kertha Wicara: Journal Ilmu Hukum*.

Rahayuda, S. (2017). Evaluasi Penggunaan Framework Laravel Pada E-government Menggunakan ISO/IEC 25010: 2011. *JURNAL IPTEKKOM (Jurnal Ilmu Pengetahuan \& Teknologi Informasi)*, *19*(1), 81–94.

Salim, A., Budiarti, R. P. N., & Yudianto, F. (2020). RANCANG BANGUN APLIKASI WEBSITE PENDAFTARAN PESERTA DIDIK BARU (PPDB) MADRASAH IBTIDAIYAH NAHDLATUL ULAMA (MINU) WARU II DENGAN MENGGUNAKAN CODEIGNITER. *NATIONAL CONFERENCE FOR UMMAH (NCU) 2020*, *1*(1).

Sandhya, S., Purkayastha, S., Joshua, E., & Deep, A. (2017). Assessment of website security by penetration testing using Wireshark. *2017 4th International Conference on Advanced Computing and Communication Systems (ICACCS)*, 1–4.

Sartika, R., Siregar, S. A. I., & Sari, N. P. R. K. (2020). Kekhususan Proses Penyidikan Tindak Pidana Cyber Crime. *Jurnal Aktual Justice*, *5*(1), 38–55.

Singh, G. D. (2019). *Learn Kali Linux 2019: Perform Powerful Penetration Testing Using Kali Linux, Metasploit, Nessus, Nmap, and Wireshark*. Packt Publishing Ltd.

Smith, B., Yurcik, W., & Doss, D. (2002). Ethical hacking: The security justification redux. *IEEE 2002 International Symposium on Technology and Society (ISTAS'02). Social Implications of Information and Communication Technology. Proceedings (Cat. No. 02CH37293)*, 374–379.

SRIDHAR, K. (n.d.). *A Technique to Enhance Information Security in Ethical Hacking*.

Subchan, M., & Setiadi, D. (2020). Information System For Sale Of Muslim Clothes Based On E-Commerce Technology: Information System For Sale Of Muslim Clothes Based On E-Commerce Technology. *Jurnal Mantik*, *4*(1), 311–318.

Sukron, M. C., Budiarti, R. P. N., & Kamil, A. S. (2020). Implementation of Nadhir Online Registration System in Badan Wakaf Indonesia Using Agile Development Methods. *Applied Technology and Computing Science*

Journal, *3*(1), 30–47.

Ushmani, A. (2018). Ethical hacking. *International Journal of Information Technology (IJIT)*, *4*(6).

Yohanie, Y., Panduman, F., Rachmat, A., Besari, A., Sukaridhoto, S., Budiarti, R. P. N., Sudibyo, R. W., & Nobuo, F. (2018). Implementation of Integration VaaMSN and SEMAR for Wide Coverage Air Quality Monitoring. *TELKOMNIKA*, *16*(6), 2630–2642. https://doi.org/10.12928/TELKOMNIKA.v16i6.10152.