Laporan Tugas Besar

Prediksi Jumlah Laporan Serta Kerugian Akibat Kejahatan Cyber (Cybercrime) Di Tahun 2021 dan Kecenderungan Pelaku Kejahatan Cyber Dalam Memilih Korbannya

Disusun untuk memenuhi Tugas Besar Mata Kuliah Literasi Data

Disusun oleh:

M. Hasyim Abdillah P.

1101191095

Jurusan Teknik Telekomunikasi

Fakultas Teknik Elektro

Universitas Telkom

Ringkasan

Perkembangan teknologi informasi yang pesat membuat kita dapat terhubung satu sama lain meskipun terpisah jarak dan waktu yang sangat jauh. Perkembangan ini memudahkan kita dalam berbagi ataupun menyimpan informasi. Namun terdapat sisi negatif dari pesatnya perkembangan teknologi informasi, yaitu munculnya berbagai tindak kejahatan yang memanfaatkan teknologi dan sistem komputer serta informasi yang kita sebut dengan kejahatan cyber (cybercrime). Motif para pelaku melakukan tindak kejahatan cyber umumnya adalah untuk kepentingan pribadi. Terdapat berbagai macam jenis kejahatan cyber namun yang paling banyak dilaporkan adalah phishing. Sasaran para pelaku kejahatan cyber mencakup semua usia dengan usia di atas 60 tahun menjadi korban yang paling banyak. Selain mencakup semua usia, kejahatan cyber juga mengincar berbagai macam sektor industri dengan sektor industri yang paling banyak mengalami kebocoran data adalah di sektor publik, kesehatan, dan finansial. Jumlah kerugian yang ditimbulkan akibat kejahatan cyber umumnya sulit untuk dikatakan secara pasti sehingga umumnya direpresentasikan dalam bentuk prediksi kerugian secara finansial.

Pendahuluan

Perkembangan teknologi membuat berbagai penyampaian informasi dapat dilakukan melalui berbagai media. Hal ini juga menyebabkan informasi dapat berasal dari mana saja dan dapat berguna untuk siapa pun. Penyimpanan data juga menjadi lebih fleksibel karena tidak harus berbentuk *hardcopy* dan dapat disimpan dengan bentuk *softcopy* pada *flashdisk* atau pun *cloud*. Menyimpan informasi atau pun data di dalam *cloud* juga dapat menghemat penggunaan kertas atau pun *hardware*. Namun dengan pesatnya perkembangan teknologi juga menyebabkan beberapa dampak negatif yang salah satunya adalah bahaya peretasan data melalui sistem informasi yang ada. Data ataupun informasi yang tersimpan di dalam *cloud* rentan untuk diretas oleh para *hacker* yang tidak bertanggung jawab. Motif para pelaku (*hacker*) melakukan peretasan dan pencurian informasi pribadi seseorang pada umumnya adalah demi keuntungan pribadi. Berbagai tindak kejahatan yang memanfaatkan sistem informasi dan komputer kita kenal dengan sebutan cybercrime.

Ada berbagai macam jenis kejahatan yang memanfaatkan sistem informasi seperti melalui dunia maya. Beberapa jenis kejahatan cybercrime yang sering terjadi adalah pemalsuan serta pencurian data atau identitas korban, *hacking*/*cracking*, dan penyalahgunaan kartu kredit. Untuk melakukan kejahatan tersebut dapat dilakukan dengan berbagai cara. Beberapa cara yang cukup terkenal di antaranya adalah *hacking*/*cracking*, *spoofing*, *DDoS attack*, dan masih banyak lainnya. Para pelaku juga memerlukan keahlian tertentu untuk dapat melakukan jenis kejahatan tersebut dalam proses cybercrime-nya. Para pelaku juga sulit untuk dilacak, sehingga pada umumnya jumlah laporan cybercrime berdasarkan laporan korbannya.

Tidak mudah untuk menangkap pelaku kejahatan cybercrime dikarenakan mereka sulit untuk dilacak. Cara terbaik adalah dengan meningkatkan kesadaran diri terhadap ancaman cybercrime. Meskipun sulit untuk menangani kasus cybercrime, tapi kita dapat menguranginya serta memperkecil risiko dengan mengetahui jenis yang sering dipakai dalam tindak kejahatan cybercrime agar tidak

menjadi korban kejahatan cyber. Dengan mengetahui jenis yang dipakai serta target para pelaku, kita dapat mengurangi dampak kerugian akibat cybercrime.

Melalui penelitian ini diharapkan dapat meningkatkan kewaspadaan kita terhadap kejahatan cyber yang dapat mengincar siapa pun di sekitar kita. Pada penelitian ini kita akan memprediksi kejahatan cyber di tahun berikutnya dari beberapa faktor seperti usia, jenis kejahatan cyber, dan sektor industri. Kita juga akan melakukan perbandingan data untuk membuktikan apakah ada perbedaan yang signifikan dari setiap faktor tersebut.

Rancangan Eksperimen dan Prosedur Penelitian

1. **Fokus Penelitian**

   Penelitian difokuskan pada rentang usia korban dan jenis yang digunakan dalam kasus kejahatan cyber (cybercrime). Selain rentang usia dan jenis yang digunakan, ada tambahan yaitu industri yang sering menjadi sasaran kejahatan cyber. Responden yang dipilih merupakan para korban kejahatan cyber, baik itu secara individu atau pun organisasi kecil hingga besar. Populasi penelitian yang dipilih berasal dari seluruh dunia, hal ini dikarenakan para korban kejahatan cyber tidak hanya berasal dari 1 negara saja, karena kita berada di zaman semua orang dapat terhubung melalui internet tanpa memedulikan jarak. Selain itu, pemilihan populasi secara global memudahkan data yang diperoleh karena ketika memfokuskan pada 1 daerah yang lebih kecil, data yang didapatkan nantinya akan terlalu sedikit.

2. **Penentuan Variabel**

   Variabel penelitian yang difokuskan adalah jumlah laporan, kerugian yang ditimbulkan, rentang usia, tahun, dan sektor industri.

3. **Pengumpulan dan Pengorganisasian Data**

   Proses pengumpulan data dilakukan melalui survei, namun karena target populasinya dari seluruh dunia maka data yang digunakan berasal dari lembaga terpercaya yang telah melakukan survei. Alasan kenapa dipilihnya jenis pengumpulan data melalui survei karena data yang diinginkan berasal dari laporan para korban kejahatan cyber. Jenis data yang dikumpulkan termasuk ke dalam data sekunder karena berasal dari organisasi lain. Sebagian besar data yang telah dikumpulkan merupakan data terstruktur dalam bentuk laporan dan data statistik. Karena data telah terorganisir, maka yang perlu dilakukan adalah memilih data yang sesuai untuk penelitian ini lalu merapikan atau mengorganisir data yang telah dipilih sesuai kebutuhan penelitian.

4. **Metodologi dan Uji Statistik**

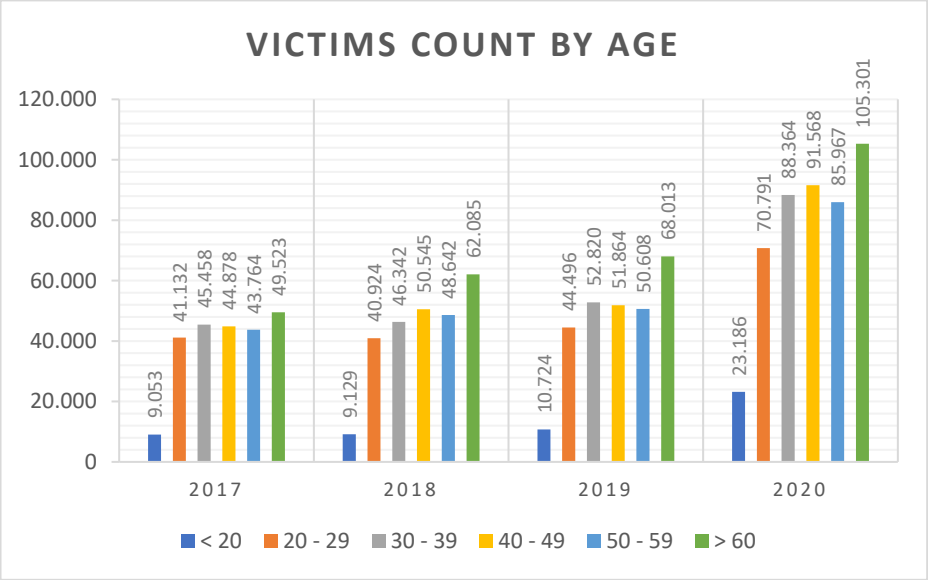
Uji statistik yang digunakan dalam penelitian ini adalah uji regresi dan ANOVA. Uji regresi dilakukan untuk melakukan prediksi jumlah laporan dan kerugian dari kejahatan cyber di tahun 2021. Uji ANOVA dilakukan untuk melihat apakah ada perbedaan yang signifikan pada data di tiap variabel penelitian.

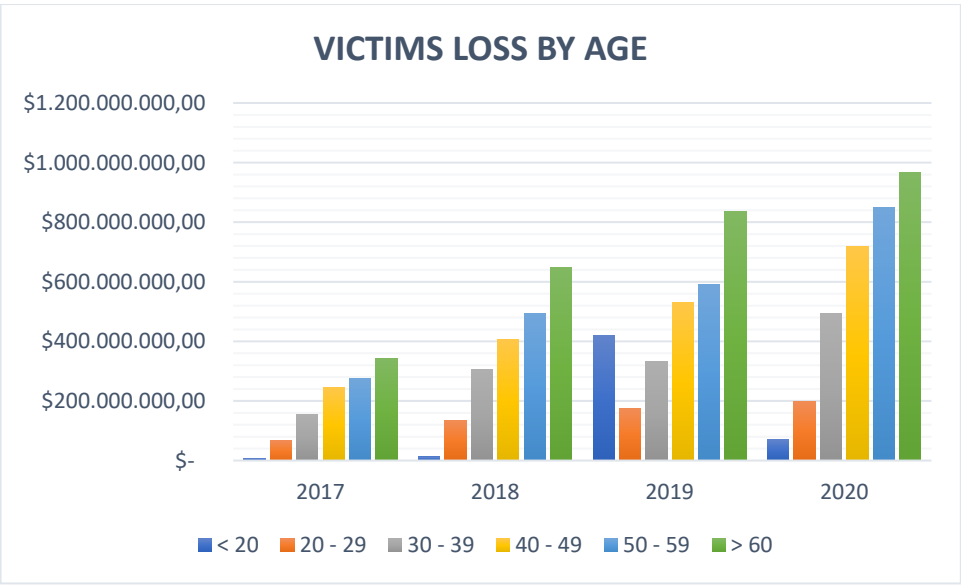
5. Pengambilan Kesimpulan

Setelah dilakukan uji statistik terhadap data yang telah dikumpulkan akan dilakukan pengambilan kesimpulan berdasarkan hasil uji statistik yang didapatkan.

Statistika Deskriptif

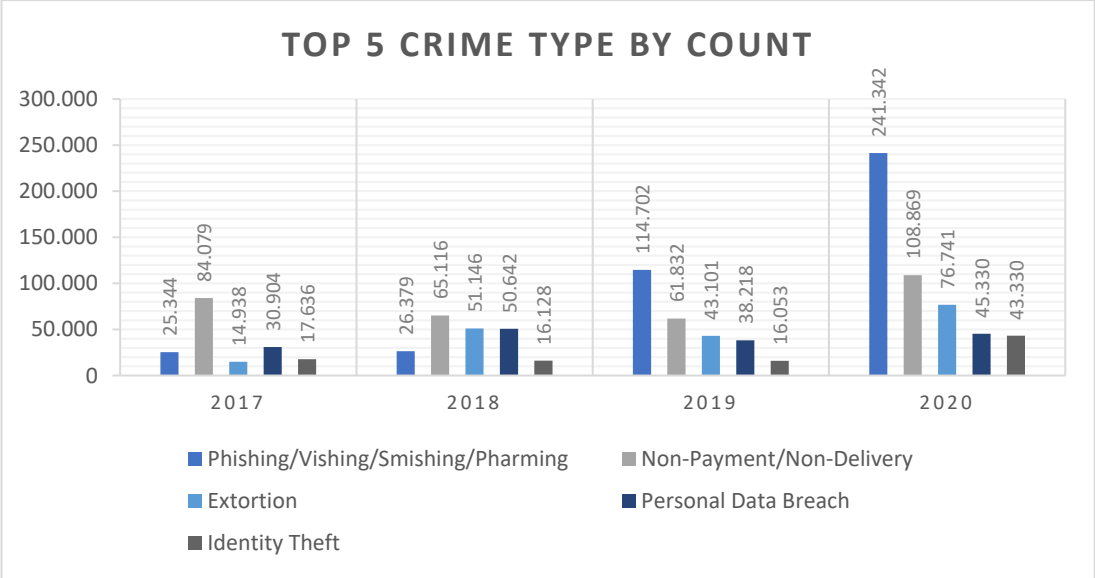
1. Berdasarkan Usia

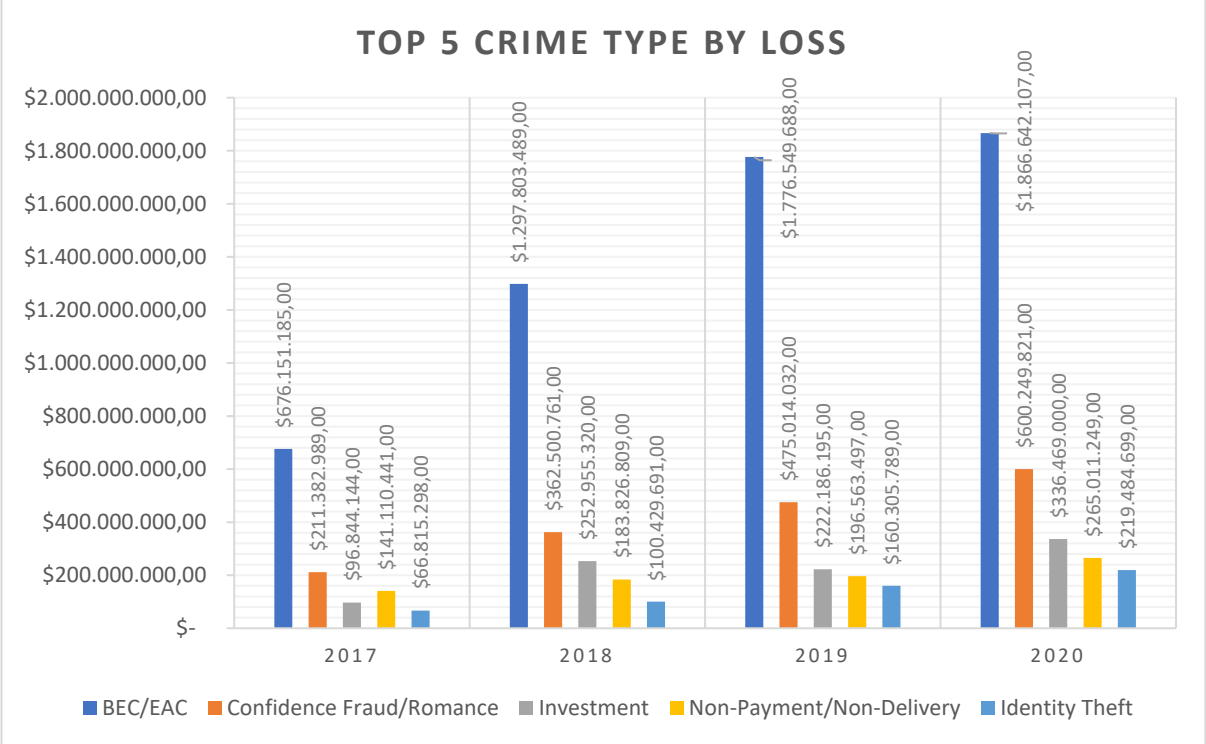




Berdasarkan 2 grafik tersebut dapat dilihat bahwa jumlah laporan dan kerugian terbanyak merupakan orang dewasa dengan usia lebih dari 60 tahun atau dapat dikategorikan sebagai lansia. Hal tersebut dikarenakan para lansia yang berusia lebih dari 60 tahun merupakan generasi yang paling sulit dalam beradaptasi dengan perkembangan teknologi sehingga mereka rentan sebagai sasaran kejahatan cyber. Dapat terlihat pula jumlah laporan serta kerugian terus meningkat setiap tahunnya pada tiap rentang usia.

2. Berdasarkan Jenis



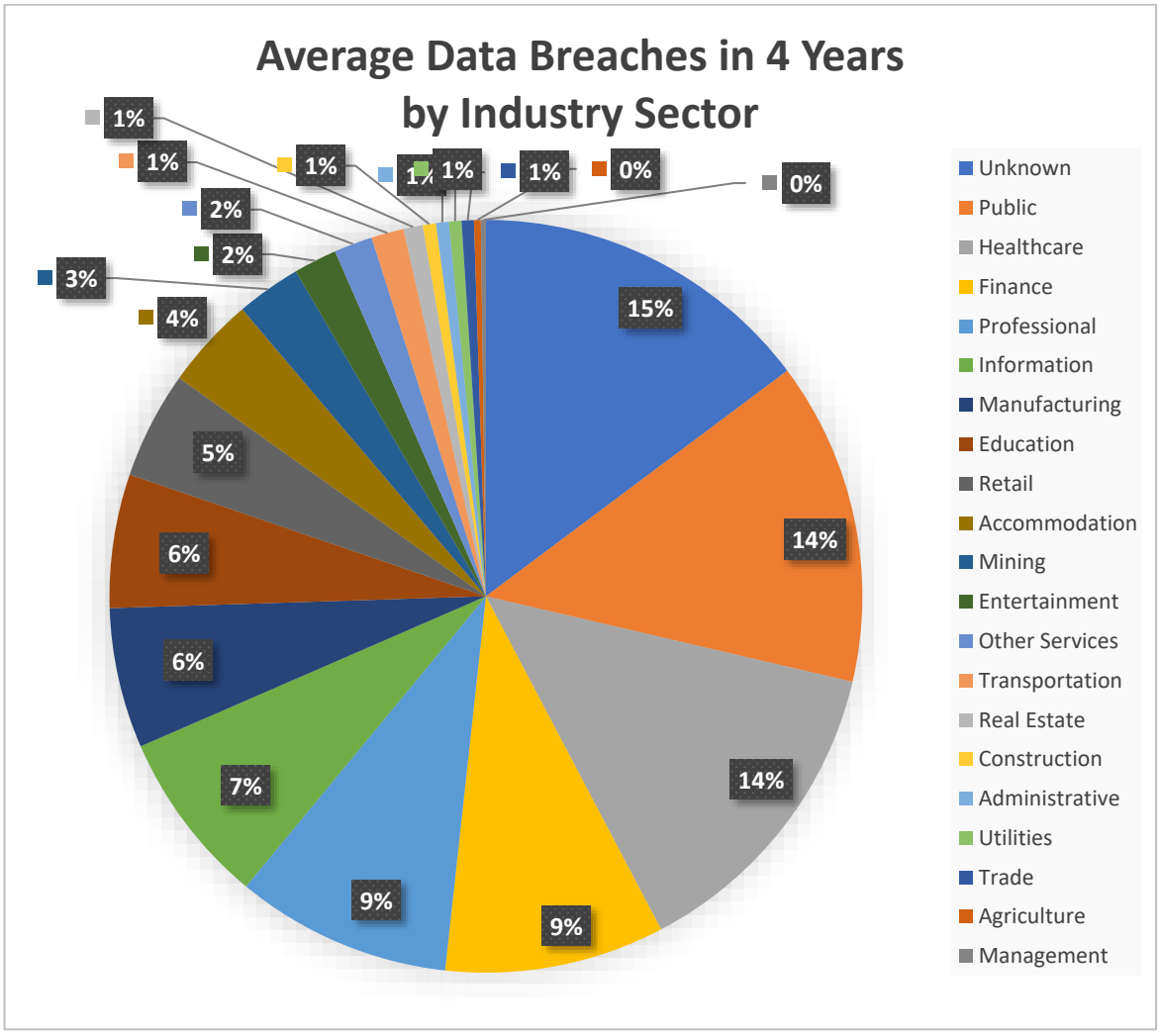


Berdasarkan grafik pertama dapat dilihat bahwa jumlah jenis yang paling sering dipakai dalam kejahatan cyber adalah *Non-Payment/Non-Delivery* (2017-2018) dan phishing (2019-2020). Dari grafik kedua dapat dilihat bahwa jumlah kerugian terbesar menggunakan jenis BAC/EAC.

Selain 10 jenis tersebut, berikut adalah keseluruhan jenis kejahatan cyber yang telah dikenali dan dilaporkan:

Phishing/Vishing/Smishing/Pharming	Employment	Corporate Data Breach
Non-Payment/Non-Delivery	Tech Support	Ransomware
Lottery/Sweepstakes/Inheritance	Real Estate/Rental	Denial of Service/TDoS
Personal Data Breach	Advanced Fee	Malware/Scareware/Virus
Government Impersonation	Identity Theft	Health Care Related
Spoofing	Overpayment	Civil Matter
Misrepresentation	Hacktivist	Re-shipping
Confidence Fraud/Romance	Investment	Charity
Harassment/Threats of Violence	Extortion	Gambling
IPR/Copyright and Counterfeit	BEC/EAC	Terrorism
Crimes Against Children	Credit Card Fraud	Other

3. Berdasarkan Industri



Dari skema di atas dapat dilihat jumlah rata-rata kebocoran data dalam 4 tahun terakhir. *Unknown* pada skema bukan berarti tidak diketahui, namun lebih tepatnya adalah tidak dapat ditentukan. Total kebocoran data dalam 4 tahun terakhir dalam skema di atas adalah 13.437 kasus dengan rata-rata 3.359 kasus per tahun.

Berikut merupakan rincian jumlah kebocoran data dari tahun 2017-2020 dari berbagai individu, organisasi kecil hingga besar:

Industry	***2017***	***2018***	***2019***	***2020***
Unknown	140	289	688	868
Public	304	330	346	885
Healthcare	536	304	521	472
Finance	146	207	448	467
Professional	132	157	326	630
Information	109	155	360	381
Manufacturing	71	87	381	270
Education	101	99	228	344
Retail	169	139	146	165
Accommodation	338	61	92	40
Mining	6	15	17	335
Entertainment	33	10	98	109
Other Services	35	54	66	67
Transportation	18	36	67	67
Real Estate	20	14	33	44
Construction	10	11	25	30
Administrative	18	17	20	19
Utilities	18	8	26	20
Trade	12	16	15	28
Agriculture	0	2	21	16
Management	0	2	26	1
Total	2216	2013	3950	5258

Metodologi/Uji Statistik

1. Prediksi Jumlah Korban di Tahun 2021

Data jumlah laporan setiap tahunnya:

Tahun	*Jumlah Korban*
2017	301.580
2018	351.937
2019	467.361
2020	791.790

Data jumlah laporan tersebut berbeda dengan jumlah korban berdasarkan usia ataupun berdasarkan jenis kejahatan cyber yang digunakan. Hal tersebut dikarenakan laporan yang diterima dari responden (korban) terkadang tidak mencantumkan usia ataupun jenis yang digunakan. Dan juga 1 laporan dapat berisi lebih dari 1 jenis atau jenis kejahatan cyber.

Uji statistik regresi:

Regression Statistics	
Multiple R	0,929463885
R Square	0,863903113
Adjusted R Square	0,79585467
Standard Error	99535,85457
Observations	4

	df	*SS*	*MS*	*F*	*Significance F*
Regression	1	1,25778E+11	1,25778E+11	12,69541332	0,070536115
Residual	2	19814772688	9907386344		
Total	3	1,45593E+11			

	Intercept	Tahun
Coefficients	-319.666.832,9	158.605,4
Standard Error	89.851.093,65	44.513,79
t Stat	-3,557740033	3,563062351
P-value	0,070725436	0,070536115
Lower 95%	-706264886,3	-32921,9689

Upper 95%	66931220,48	350132,7689
Lower 95,0%	-706264886,3	-32921,9689
Upper 95,0%	66931220,48	350132,7689

Dari uji statistik didapat persamaan berikut:

$$Jumlah\ laporan = [-319.666.832{,}9 + (tahun \times 158.605{,}4)]$$

Prediksi jumlah laporan di tahun 2021 sebanyak:

$$Jumlah\ laporan = [-319.666.832{,}9 + (2021 \times 158.605{,}4)] = 874.681 \text{ laporan}$$

Prediksi laporan terkait kejahatan cyber kemungkinan akan mencapai 874.681 laporan di tahun 2021.

2. Prediksi Kerugian di Tahun 2021

Data jumlah kerugian yang dilaporkan setiap tahunnya:

Tahun	***Jumlah kerugian***
2017	$ 1.426.668.409,00
2018	$ 2.709.160.726,00
2019	$ 3.633.089.225,50
2020	$ 4.169.074.294,00

Uji statistik regresi:

Regression Statistics	
Multiple R	0,983762745
R Square	0,967789139
Adjusted R Square	0,951683708
Standard Error	263971045,9
Observations	4

	df	*SS*	*MS*	*F*	*Significance F*
Regression	1	4,18717E+18	4,18717E+18	60,09085748	0,016237255
Residual	2	1,39361E+17	6,96807E+16		
Total	3	4,32654E+18			

	Intercept	Tahun
Coefficients	-1,84417E+12	915114615,5

Standard Error	2,38287E+11	118051440,5
t Stat	-7,739303298	7,751829299
P-value	0,016288579	0,016237255
Lower 95%	-2,86944E+12	407180262,6
Upper 95%	-8,18909E+11	1423048968
Lower 95,0%	-2,86944E+12	407180262,6
Upper 95,0%	-8,18909E+11	1423048968

Dari uji statistik didapatkan persamaan:

$$Jumlah\ kerugian = (-1{,}84417 \times 10^{12}) + (tahun \times 915.114.615{,}5)$$

Prediksi jumlah kerugian di tahun 2021:

$$Jumlah\ kerugian = (-1{,}84417 \times 10^{12}) + (2021 \times 915.114.615{,}5)$$
$$= USD\ 5.272.284.702{,}25$$

Prediksi kerugian akibat kejahatan cyber kemungkinan akan mencapai USD 5.272.284.702,25 di tahun 2021.

3. Perbedaan Antar Kelompok Variabel

Uji statistik kali ini menggunakan uji ANOVA dengan membandingkan data antar kelompok dan melihat apakah ada perbedaan yang signifikan. Kelompok variabel yang dipilih adalah rentang usia, jenis, dan sektor industri.

a. Kelompok rentang usia

Data berdasarkan variabel usia:

Age	***2017***	***2018***	***2019***	***2020***
< 20	9.053	9.129	10.724	23.186
20 - 29	41.132	40.924	44.496	70.791
30 - 39	45.458	46.342	52.820	88.364
40 - 49	44.878	50.545	51.864	91.568
50 - 59	43.764	48.642	50.608	85.967
> 60	49.523	62.085	68.013	105.301
Total	233.808	257.667	278.525	465.177

Uji statistik ANOVA:

SUMMARY	*Count*	*Sum*	*Average*	*Variance*

< 20	4	52.092	13.023,00	46.498.702,00
20 - 29	4	197.343	49.335,75	207.269.994,92
30 - 39	4	232.984	58.246,00	413.924.520,00
40 - 49	4	238.855	59.713,75	460.159.090,92
50 - 59	4	228.981	57.245,25	374.917.340,92
> 60	4	284.922	71.230,50	575.335.667,67
2017	6	233.808	38.968,00	222.209.592,40
2018	6	257.667	42.944,50	323.140.262,70
2019	6	278.525	46.420,83	366.460.063,37
2020	6	465.177	77.529,50	831.107.373,10

Source of Variation	Rows	Columns	Error	Total
SS	8.081.724.738	5.601.454.229	632.861.720	14.316.040.687
df	5	3	15	23
MS	1.616.344.948	1.867.151.410	42.190.781	
F	38,31038194	44,255		
P-value	5,05555E-08	1E-07		
F crit	2,901294536	3,2874		

$H_0 = tidak\ terdapat\ perbedaan\ yang\ signifikan$

$H_1 = terdapat\ perbedaan\ yang\ signifikan$

Dari uji statistik didapat nilai $p = 5 \times 10^{-8}$ pada kelompok usia. Karena $p < 0{,}05$, maka H_0 ditolak dan H_1 diterima, yang artinya terdapat perbedaan yang signifikan antar usia.

Berdasarkan hasil uji statistik tersebut dapat diambil kesimpulan bahwa pelaku kejahatan cyber lebih memilih rentang usia tertentu sebagai sasaran dari kejahatan mereka. Dari data dapat terlihat rentang usia yang paling sering menjadi sasaran adalah lebih dari 60 tahun ($>$ 60) dan yang paling jarang diincar adalah mereka dengan rentang usia kurang dari 20 tahun.

b. Kelompok jenis

Data berdasarkan variabel jenis:

Crime Type	***2017***	***2018***	***2019***	***2020***
Advanced Fee	16.368	16.362	14.607	13.020
BEC/EAC	15.690	20.373	23.775	19.369
Charity	436	493	407	659

Civil Matter	1.057	768	908	968
Confidence Fraud/Romance	15.372	18.493	19.473	23.751
Corporate Data Breach	3.785	2.480	1.795	2.794
Credit Card Fraud	15.220	15.212	14.378	17.614
Crimes Against Children	1.300	1.394	1.312	3.202
Denial of Service/TDoS	1.201	1.799	1.353	2.018
Employment	15.784	14.979	14.493	16.879
Extortion	14.938	51.146	43.101	76.741
Gambling	203	181	262	391
Government Impersonation	9.149	10.978	13.873	12.827
Hacktivist	158	77	39	52
Harassment/Threats of Violence	16.194	18.415	15.502	20.604
Health Care Related	406	337	657	1.383
Identity Theft	17.636	16.128	16.053	43.330
Investment	3.089	3.693	3.999	8.788
IPR/Copyright and Counterfeit	2.644	2.249	3.892	4.213
Lottery/Sweepstakes/Inheritance	3.012	7.146	7.767	8.501
Malware/Scareware/Virus	3.089	2.811	2.373	1.423
Misrepresentation	5.437	5.959	5.975	24.276
No Lead Value	20.241	36.936	0	0
Non-Payment/Non-Delivery	84.079	65.116	61.832	108.869
Other	14.023	10.826	10.842	10.372
Overpayment	23.135	15.512	15.395	10.988
Personal Data Breach	30.904	50.642	38.218	45.330
Phishing/Vishing/Smishing/Pharming	25.344	26.379	114.702	241.342
Ransomware	1.783	1.493	2.047	2.474
Real Estate/Rental	9.645	11.300	11.677	13.638
Re-shipping	1.025	907	929	883
Spoofing	0	15.569	25.789	28.218
Tech Support	10.949	14.408	13.633	15.421
Terrorism	177	120	61	65
Total	383.473	460.681	501.119	780.403

Uji statistik ANOVA:

SUMMARY	*Count*	*Sum*	*Average*	*Variance*
Advanced Fee	4	60.357	15.089	2.589.818
BEC/EAC	4	79.207	19.802	11.068.934
Charity	4	1.995	499	12.690
Civil Matter	4	3.701	925	14.737
Confidence Fraud/Romance	4	77.089	19.272	11.972.894
Corporate Data Breach	4	10.854	2.714	684.252
Credit Card Fraud	4	62.424	15.606	1.948.093
Crimes Against Children	4	7.208	1.802	872.856
Denial of Service/TDoS	4	6.371	1.593	144.775

Employment		4	62.135	15.534	1.087.744
Extortion		4	185.926	46.482	647.938.358
Gambling		4	1.037	259	8.884
Government Impersonation		4	46.827	11.707	4.340.254
Hacktivist		4	326	82	2.850
Harassment/Threats of Violence		4	70.715	17.679	5.347.292
Health Care Related		4	2.783	696	228.824
Identity Theft		4	93.147	23.287	179.079.229
Investment		4	19.569	4.892	6.888.225
IPR/Copyright and Counterfeit		4	12.998	3.250	902.923
Lottery/Sweepstakes/Inheritance		4	26.426	6.607	6.049.127
Malware/Scareware/Virus		4	9.696	2.424	532.199
Misrepresentation		4	41.647	10.412	85.492.433
No Lead Value		4	57.177	14.294	318.887.948
Non-Payment/Non-Delivery		4	319.896	79.974	467.221.459
Other		4	46.063	11.516	2.841.387
Overpayment		4	65.030	16.258	25.455.771
Personal Data Breach		4	165.094	41.274	73.695.532
Phishing/Vishing/Smishing/Pharming		4	407.767	101.942	10.390.732.724
Ransomware		4	7.797	1.949	173.574
Real Estate/Rental		4	46.260	11.565	2.688.833
Re-shipping		4	3.744	936	3.873
Spoofing		4	69.576	17.394	164.505.621
Tech Support		4	54.411	13.603	3.665.922
Terrorism		4	423	106	2.981
	2017	34	383.473	11.279	239.252.811
	2018	34	460.681	13.549	257.669.792
	2019	34	501.119	14.739	505.005.569
	2020	34	780.403	22.953	2.016.355.377

Source of Variation	Rows	Columns	Error	Total
SS	64.993.372.943,88	2.641.264.876,94	34.609.984.163,06	1,02E+11
df	33	3	99	135
MS	1.969.496.149,81	880.421.625,65	349.595.799,63	
F	5,63363791	2,518398752		
P-value	1,11426E-11	0,062446807		
F crit	1,553940151	2,696468997		

$$H_0 = tidak\ terdapat\ perbedaan\ yang\ signifikan$$

$$H_1 = terdapat\ perbedaan\ yang\ signifikan$$

Dari uji statistik didapat nilai $p = 1{,}11 \times 10^{-11}$ pada kelompok jenis. Karena $p < 0{,}05$, maka H_0 ditolak dan H_1 diterima, yang artinya terdapat perbedaan yang signifikan antar jenis.

Berdasarkan hasil uji statistik tersebut dapat diambil kesimpulan bahwa pelaku kejahatan cyber lebih memilih jenis kejahatan cyber tertentu dalam melakukan aksi kejahatannya. Faktor pemilihan jenis kejahatan cyber umumnya adalah tingkat kesulitan dan keberhasilan jenis tersebut, dan tujuan yang ingin dicapai dari pelaku. Dari data dapat dilihat bahwa yang paling sering dilaporkan adalah phishing dan yang paling jarang adalah *hacktivist*.

c. Kelompok sektor industri

Data berdasarkan variabel sektor industri:

Industry	*2017*	*2018*	*2019*	*2020*
Unknown	140	289	688	868
Public	304	330	346	885
Healthcare	536	304	521	472
Finance	146	207	448	467
Professional	132	157	326	630
Information	109	155	360	381
Manufacturing	71	87	381	270
Education	101	99	228	344
Retail	169	139	146	165
Accommodation	338	61	92	40
Mining	6	15	17	335
Entertainment	33	10	98	109
Other Services	35	54	66	67
Transportation	18	36	67	67
Real Estate	20	14	33	44
Construction	10	11	25	30
Administrative	18	17	20	19
Utilities	18	8	26	20
Trade	12	16	15	28
Agriculture	0	2	21	16
Management	0	2	26	1
Total	2216	2013	3950	5258

Uji statistik ANOVA:

SUMMARY	*Count*	*Sum*	*Average*	*Variance*

Unknown	4	1985	496,25	114.944,25000
Public	4	1865	466,25	78.233,58333
Healthcare	4	1833	458,25	11.321,58333
Finance	4	1268	317	27.000,66667
Professional	4	1245	311,25	52.580,91667
Information	4	1005	251,25	19.386,91667
Manufacturing	4	809	202,25	22.350,25000
Education	4	772	193	13.775,33333
Retail	4	619	154,75	210,91667
Accommodation	4	531	132,75	19.179,58333
Mining	4	373	93,25	25.997,58333
Entertainment	4	250	62,5	2.349,66667
Other Services	4	222	55,5	221,66667
Transportation	4	188	47	587,33333
Real Estate	4	111	27,75	180,25000
Construction	4	76	19	100,66667
Administrative	4	74	18,5	1,66667
Utilities	4	72	18	56,00000
Trade	4	71	17,75	49,58333
Agriculture	4	39	9,75	106,91667
Management	4	29	7,25	156,91667
2017	21	2216	105,5238095	18.905,2619
2018	21	2013	95,85714286	11.464,12857
2019	21	3950	188,0952381	40.394,99048
2020	21	5258	250,3809524	78.043,14762

Source of Variation	Rows	Columns	Error	Total
SS	2.146.614,143	336.840,321	829.536,429	3.312.990,893
df	20	3	60	83
MS	107.330,707	112.280,107	13.825,607	
F	7,76318219	8,12		
P-value	2,85253E-10	0		
F crit	1,747984133	2,76		

$H_0 = tidak\ terdapat\ perbedaan\ yang\ signifikan$

$H_1 = terdapat\ perbedaan\ yang\ signifikan$

Dari uji statistik didapat nilai $p = 2{,}8 \times 10^{-10}$ pada kelompok jenis. Karena $p < 0{,}05$, maka H_0 ditolak dan H_1 diterima, yang artinya terdapat perbedaan yang signifikan antar sektor industri.

Berdasarkan hasil uji statistik tersebut dapat diambil kesimpulan bahwa pelaku kejahatan cyber lebih memilih sektor industri tertentu sebagai sasaran dari kejahatan mereka. Jika kita mengecualikan *unknown*, dari data terlihat bahwa sektor industri yang paling sering diincar adalah sektor publik dan yang paling jarang adalah manajemen.

Hasil dan Kesimpulan

Berdasarkan hasil uji statistik pada data dan melihat kecenderungan data jumlah laporan yang diterima dari tahun ke tahun, dapat disimpulkan bahwa jumlah laporan terkait kejahatan cyber akan terus meningkat setiap tahunnya dengan prediksi sebanyak 874.681 laporan di tahun 2021. Dari hasil uji statistik juga dapat diprediksikan bahwa kerugian akibat kejahatan cyber akan mencapai USD 5.272.284.702,25 di tahun 2021. Melihat kecenderungan data yang terus meningkat di setiap tahunnya maka dapat disimpulkan bahwa jumlah laporan dan kerugian akibat kejahatan cyber masih akan terus meningkat di tahun berikutnya.

Para pelaku kejahatan cyber tidak memilih korbannya secara acak, namun mereka memiliki kecenderungan tertentu dalam memilih korbannya. Pelaku kejahatan cyber cenderung memilih korban dengan usia di atas 60 tahun yaitu para lansia. Alasan yang paling mungkin mengapa mereka memilih korban dengan usia di atas 60 tahun karena orang-orang lansia pada umumnya yang paling sulit beradaptasi dengan perkembangan teknologi sehingga mereka yang paling rentan menjadi korban kejahatan cyber.

Selain menyerang secara individu, para pelaku kejahatan cyber juga menyerang berbagai organisasi dari skala kecil hingga besar. Organisasi yang paling sering menjadi korban kejahatan cyber berada di sektor publik, Kesehatan, dan finansial. Alasan yang paling mungkin mengapa para pelaku menyerang 3 sektor tersebut karena ketiga sektor tersebut memiliki prospek yang paling menguntungkan bagi pelaku.

Setelah pelaku menentukan sasaran korbannya, selanjutnya mereka memilih jenis kejahatan cyber yang akan dilakukan. Jenis kejahatan cyber secara tidak langsung juga merupakan metode para pelaku untuk menyerang korbannya. Jenis kejahatan cyber yang paling sering digunakan adalah phishing. Para pelaku memilih menggunakan jenis kejahatan phishing karena merupakan metode yang paling mudah untuk dilakukan dibandingkan jenis yang lainnya.

Diskusi

1. Apa dampak dari cybercrime bagi sebuah perusahaan besar?

   Jawaban: ada berbagai dampak negatif dari cybercrime bagi sebuah perusahaan mulai dari kehilangan data, kerugian finansial, hingga bocornya rahasia perusahaan. Secara umum dampak buruk ini dilaporkan sebagai bentuk kerugian finansial. Untuk kerugian berupa hilang atau bocornya data ke pihak luar dilakukan pula prediksi kerugiannya secara finansial.

2. Hal apa yang bisa dilakukan oleh sebuah perusahaan agar dapat mengurangi dampak cybercrime?

   Jawaban: secanggih apa pun sistem keamanan cyber yang dimiliki suatu perusahaan akan selalu ada celah bagi para pelaku untuk melakukan tindak kejahatan cyber. Hal yang dapat dilakukan untuk meminimalkan dampaknya adalah dengan melakukan pembaruan sistem keamanan secara berkala dan meningkatkan kewaspadaan karyawan terhadap ancaman kejahatan cyber.

3. Berikan penjelasan tentang sumber data yang digunakan dalam penelitian ini!

   Jawaban: data yang dikumpulkan sebagian besar berasal dari situs milik statista. Setelah masuk ke situs statista dilanjutkan dengan pencarian data relevan dengan yang dibutuhkan untuk penelitian. Data yang disediakan oleh statista berupa tampilan statistik data beserta referensinya. Dikarenakan data yang ditampilkan oleh statista hanya sebagian maka saya melakukan riset lebih lanjut dengan menelusuri sumber referensi. Referensi tambahan setelah dari statista adalah dari IC3 FBI dan Verizon.

4. Apakah tidak ada kemungkinan bahwa ada tahun di mana kasus kejahatan cyber menurun?

   Jawaban: ada kemungkinan kasus kejahatan cyber dapat menurun di tahun berikutnya. Berdasarkan hasil uji regresi di uji statistik didapat

kemungkinan hasil uji tidak sesuai dengan yang didapat adalah 5%-7%. Jadi kemungkinan bahwa jumlah kasus kejahatan cyber akan menurun di tahun berikutnya sebesar 5%-7%.

5. Mengapa sulit melacak pelaku kejahatan cyber?

   Jawaban: para pelaku akan melakukan persiapan sebelum melancarkan aksinya, mulai dari menggunakan VPN, memakai browser khusus, terkadang menggunakan perangkat laptop atau PC tersendiri, dan lain-lain agar tidak dapat dilacak keberadaannya

Glosarium

Overpayment	Seseorang dikirimi pembayaran/komisi dan diperintahkan untuk menyimpan sebagian dari pembayaran dan mengirimkan sisanya ke individu atau bisnis lain.
Advanced Fee	Seorang individu membayar uang kepada seseorang untuk mengantisipasi menerima sesuatu yang bernilai lebih besar sebagai imbalannya, tetapi sebaliknya, menerima jauh lebih sedikit dari yang diharapkan atau tidak sama sekali.
Business Email Compromise/Email Account Compromise (BEC/EAC)	BEC adalah bisnis penargetan scam (bukan individu) yang bekerja dengan pemasok asing dan/atau bisnis yang secara teratur melakukan pembayaran transfer kawat. EAC adalah penipuan serupa yang menargetkan individu. Penipuan canggih ini dilakukan oleh penipu yang mengkompromikan akun email melalui rekayasa sosial atau teknik intrusi komputer untuk melakukan transfer dana yang tidak sah.
Charity	Pelaku membuat amal palsu, biasanya setelah bencana alam, dan mendapat untung dari individu yang percaya bahwa mereka memberikan sumbangan ke organisasi amal yang sah.
Civil Matter	Litigasi perdata umumnya mencakup semua perselisihan yang secara resmi diajukan ke pengadilan, tentang subjek apa pun di mana satu pihak diklaim telah melakukan kesalahan tetapi bukan kejahatan. Secara umum, ini adalah proses hukum yang kebanyakan orang pikirkan ketika kata “gugatan” digunakan.
Confidence/Romance Fraud	Seseorang percaya bahwa mereka berada dalam suatu hubungan (keluarga, persahabatan, atau romantis) dan ditipu untuk mengirim uang, informasi pribadi dan keuangan, atau barang berharga kepada pelaku atau untuk mencuci uang atau barang untuk membantu pelaku. Ini termasuk Skema Kakek-Nenek dan skema apa pun di mana pelaku memangsa "hati" pengadu.
Corporate Data Breach	Kebocoran atau tumpahan data bisnis yang dilepaskan dari lokasi yang aman ke lingkungan yang tidak tepercaya. Ini juga dapat merujuk pada pelanggaran data dalam perusahaan atau bisnis di mana data sensitif, dilindungi, atau rahasia disalin, dikirim, dilihat, dicuri, atau digunakan oleh individu yang tidak berwenang untuk melakukannya.
Credit Card Fraud	Penipuan kartu kredit adalah istilah luas untuk pencurian dan penipuan yang dilakukan

	menggunakan kartu kredit atau mekanisme pembayaran serupa (ACH. EFT, biaya berulang, dll.) sebagai sumber penipuan dana dalam suatu transaksi.
Crimes Against Children	Segala sesuatu yang berhubungan dengan eksploitasi anak, termasuk kekerasan terhadap anak.
Denial of Service/TDoS	Serangan Denial of Service (DoS) membanjiri jaringan/sistem atau Telephony Denial of Service (TDoS) membanjiri layanan suara dengan banyak permintaan, memperlambat atau mengganggu layanan.
Employment	Seseorang percaya bahwa mereka dipekerjakan secara sah dan kehilangan uang, atau mencuci uang/barang selama masa kerja mereka.
Extortion	Pengambilan uang atau properti secara tidak sah melalui intimidasi atau penggunaan wewenang yang tidak semestinya. Ini mungkin termasuk ancaman bahaya fisik, tuntutan pidana, atau paparan publik.
Gambling	Perjudian online, juga dikenal sebagai perjudian Internet dan iGambling, adalah istilah umum untuk perjudian menggunakan Internet.
Government Impersonation	Seorang pejabat pemerintah menyamar dalam upaya untuk mengumpulkan uang.
Hacktivist	Seorang *hacker* komputer yang aktivitasnya ditujukan untuk mempromosikan tujuan sosial atau politik.
Harassment/Threats of Violence	Pelecehan terjadi ketika pelaku menggunakan tuduhan palsu atau pernyataan fakta untuk mengintimidasi korban. Ancaman Kekerasan mengacu pada ekspresi niat untuk menimbulkan rasa sakit, cedera, atau hukuman, yang tidak mengacu pada persyaratan pembayaran.
Health Care Related	Skema yang mencoba menipu program perawatan kesehatan swasta atau pemerintah yang biasanya melibatkan penyedia layanan kesehatan, perusahaan, atau individu. Skema dapat mencakup penawaran untuk kartu asuransi palsu, bantuan pasar asuransi kesehatan, informasi kesehatan yang dicuri, atau berbagai penipuan lain dan/atau skema apa pun yang melibatkan obat-obatan, suplemen, produk penurun berat badan, atau praktik pengalihan/pabrik pil. Penipuan ini sering dimulai melalui email spam, iklan Internet, tautan di forum/media sosial, dan situs web penipuan.
IPR/Copyright and Counterfeit	Pencurian ilegal dan penggunaan ide, penemuan, dan ekspresi kreatif orang lain – yang disebut kekayaan intelektual – semuanya mulai dari rahasia dagang dan produk serta suku cadang berpemilik hingga film, musik, dan perangkat lunak.

Identity Theft	Seseorang mencuri dan menggunakan informasi pengenal pribadi, seperti nama atau nomor Jaminan Sosial, tanpa izin untuk melakukan penipuan atau kejahatan lainnya dan/atau (Pengambilalihan Akun) penipu memperoleh informasi akun untuk melakukan penipuan pada akun yang ada.
Investment	Praktik penipuan yang mendorong investor untuk melakukan pembelian atas dasar informasi palsu. Penipuan ini biasanya menawarkan pengembalian besar kepada korban dengan risiko minimal. (Pensiun, 401K, Ponzi, Piramida, dll.).
Lottery/Sweepstakes/ Inheritance	Seseorang dihubungi tentang memenangkan lotre atau undian yang tidak pernah mereka ikuti, atau untuk mengumpulkan warisan dari kerabat yang tidak dikenal.
Malware/Scareware/Virus	Perangkat lunak atau kode yang dimaksudkan untuk merusak, melumpuhkan, atau mampu menggandakan dirinya sendiri ke dalam komputer dan/atau sistem komputer untuk memberikan efek yang merugikan atau menghancurkan data.
Misrepresentation	Barang dagangan atau layanan dibeli atau dikontrak oleh individu secara online yang pembayarannya diberikan oleh pembeli. Barang atau jasa yang diterima memiliki kualitas atau kuantitas yang jauh lebih rendah daripada yang dijelaskan oleh penjual.
No Lead Value	Pengaduan yang tidak lengkap yang tidak memungkinkan untuk menentukan jenis kejahatan.
Non-Payment/Non-Delivery	Dalam situasi non-pembayaran, barang dan jasa dikirim, tetapi pembayaran tidak pernah diberikan. Dalam situasi non-pengiriman, pembayaran dikirim, tetapi barang dan jasa tidak pernah diterima.
Personal Data Breach	Kebocoran/tumpahan data pribadi yang dilepaskan dari lokasi yang aman ke lingkungan yang tidak terpercaya. Juga, insiden keamanan di mana data sensitif, dilindungi, atau rahasia seseorang disalin, dikirim, dilihat, dicuri, atau digunakan oleh individu yang tidak berwenang.
Phishing/Vishing/Smishing/ Pharming	Penggunaan email, pesan teks, dan panggilan telepon yang tidak diminta yang konon dari perusahaan sah yang meminta kredensial pribadi, keuangan, dan/atau login.
Ransomware	Jenis perangkat lunak berbahaya yang dirancang untuk memblokir akses ke sistem komputer hingga uang dibayarkan.
Re-shipping	Individu menerima paket di tempat tinggal mereka dan kemudian mengemas ulang barang dagangan untuk pengiriman, biasanya ke luar negeri.

Real Estate/Rental	Kehilangan dana dari investasi real estate atau penipuan yang melibatkan sewa atau properti timeshare.
Spoofing	Informasi kontak (nomor telepon, email, dan situs web) sengaja dipalsukan untuk menyesatkan dan seolah-olah berasal dari sumber yang sah. Misalnya, nomor telepon palsu yang membuat panggilan robot massal; email palsu mengirim spam massal; situs web palsu yang digunakan untuk menyesatkan dan mengumpulkan informasi pribadi. Sering digunakan sehubungan dengan jenis kejahatan lainnya.
Social Media	Pengaduan yang menuduh penggunaan jejaring sosial atau media sosial (Facebook, Twitter, Instagram, chat room, dll) sebagai vektor penipuan. Media Sosial tidak termasuk situs kencan.
Tech Support	Subjek menyamar sebagai dukungan/layanan teknis atau pelanggan.
Terrorism	Tindakan kekerasan yang dimaksudkan untuk menciptakan ketakutan yang dilakukan untuk tujuan agama, politik, atau ideologis dan dengan sengaja menargetkan atau mengabaikan keselamatan non-pejuang.
Virtual Currency	Keluhan yang menyebutkan bentuk cryptocurrency virtual, seperti Bitcoin, Litecoin, atau Potcoin.