Pengetahuan dan Kemampuan yang Dimiliki Pengguna Non-Ahli dalam Mendeteksi Phishing

IEEE Publication Technology, *Adhi Wahyu Utama and Dimas Anwar Aziz, Telkom University,*

***Abstract*—Email phishing adalah komunikasi penipuan yang berpura-pura menjadi sesuatu yang bukan sebenarnya untuk membuat orang melakukan tindakan yang seharusnya tidak mereka lakukan. Kami melakukan survei terhadap beberapa orang dari berbagai demografi di Indonesia dan meminta mereka untuk berbagi pengalaman mereka terkait email phishing. Dari analisis pengalaman tersebut, kami menemukan bahwa cara pengguna email mendeteksi pesan phishing memiliki banyak kesamaan dengan cara ahli IT mengidentifikasi phishing. Kami juga menemukan bahwa pengguna email memiliki pengetahuan unik dan kemampuan berharga dalam proses identifikasi yang tidak dimiliki oleh kontrol teknis maupun ahli IT. Kami menyarankan bahwa pelatihan yang ditargetkan pada cara memanfaatkan keunikan ini kemungkinan akan meningkatkan pencegahan phishing.**

***Index Terms*—Phishing detection, non-expert users, email security, user capabilities, cybersecurity awareness, security training, user knowledge, online threats, digital literacy, human factors in security.**

I. Introduction

EMAIL adalah salah satu metode komunikasi yang paling umum digunakan, terutama dalam organisasi besar dan e-commerce. Lebih dari 3,9 miliar orang memiliki akun email, dan secara kolektif mereka mengirim dan menerima lebih dari 290 miliar email per hari [1]. Email merupakan salah satu metode utama yang digunakan untuk berkomunikasi dengan orang asing. Namun, karena email adalah sistem global di mana siapa saja dapat berkomunikasi dengan siapa saja, pelaku kejahatan mengirim email yang berpura-pura menjadi sesuatu yang bukan sebenarnya, dan menipu orang untuk melakukan tindakan yang seharusnya tidak mereka lakukan — yang dikenal sebagai phishing [2]. Pesan phishing adalah vektor serangan yang telah menyebabkan banyak kerugian dalam masyarakat. Email phishing telah digunakan untuk mencuri uang dalam jumlah besar [3], menginstal ransomware [4], atau sekadar mencuri konten email yang kemudian dipublikasikan [5]. 32% dari semua pelanggaran perusahaan pada tahun 2018 disebabkan oleh phishing [6]. Spear-phishing – varian di mana email disesuaikan khusus dengan penerima – digunakan oleh 65% kelompok yang melakukan serangan siber yang ditargetkan, dan lebih umum digunakan daripada kerentanan zero-day (hanya 23% dari kelompok tersebut) [7].

Phishing adalah masalah sosio-teknis, dan menangani masalah ini membutuhkan kerja sama antara inovasi teknologi dan intervensi manusia. Teknologi sedang dikembangkan untuk membantu mengidentifikasi dan menyaring pesan phishing, tetapi teknologi ini tidak bekerja dengan akurasi 100% dan dapat lambat merespons inovasi baru oleh penyerang [8]. Administrator IT dan pemerintah sering mencoba menghentikan phishing sebelum dimulai dengan mengganggu situs web phishing dan pengiriman email massal [9]. Tetapi garis pertahanan terakhir adalah pengguna akhir; pesan phishing yang melewati pertahanan lain masih dapat dideteksi atau diabaikan oleh pengguna akhir untuk mencegah kerugian.

Dalam penelitian ini, kami mensurvei pengguna email tanpa pelatihan atau keahlian IT dan menanyakan mereka tentang pengalaman spesifik dengan email phishing yang mereka terima. Sekitar setengah dari responden survei dapat mengidentifikasi insiden spesifik yang kemudian mereka jawab dengan pertanyaan terperinci. Berdasarkan model Wash [2] tentang bagaimana ahli IT mendeteksi email phishing, kami menanyakan setiap orang tentang apa yang mereka perhatikan dari email tersebut, apa yang mereka harapkan dalam email tersebut, apa yang membuat mereka curiga terhadap email tersebut, investigasi apa yang mereka lakukan, bagaimana mereka memutuskan apakah email tersebut sah, dan apa yang akhirnya mereka lakukan dengan email tersebut.

Dari pertanyaan-pertanyaan ini, kami dapat mengidentifikasi pola bagaimana pengguna email yang bukan ahli IT saat ini mengidentifikasi email penipuan phishing di kotak masuk mereka. Sebagian besar penelitian melihat kegagalan deteksi phishing dan apa yang perlu diperbaiki; sebaliknya kami membandingkan non-ahli dengan para ahli Wash dan mengidentifikasi apa yang berhasil dengan baik yang dapat kita kembangkan. Kami menemukan bahwa pengguna email sering membawa pengetahuan unik ke proses identifikasi ini yang tidak dimiliki oleh metode pencegahan phishing lainnya, seperti apakah email tersebut diharapkan atau tidak dan seperti apa email seperti ini biasanya terlihat dan meminta. Kami juga menemukan bahwa pengguna email memiliki kemampuan berharga untuk investigasi, seperti meminta saran dari orang lain, atau memeriksa keabsahan dengan pengirim. Secara keseluruhan, temuan ini menunjukkan bahwa pengguna email dapat menjadi bagian penting dari ekosistem pencegahan phishing, meskipun pelatihan phishing dapat ditingkatkan untuk fokus pada bagaimana pengguna dapat lebih baik menggunakan pengetahuan dan kemampuan unik mereka.

II. Previous Work

A. Mencegah Bahaya dari Phishing

Masyarakat kita memiliki tiga bentuk pertahanan yang membantu mengidentifikasi dan membatasi keberhasilan penipuan phishing. Pertahanan teknologi mencoba secara otomatis mendeteksi fitur-fitur yang diketahui dari email phishing dan memblokir atau menghapus email tersebut. Beber-

This paper was produced by the IEEE Publication Technology Group. They are in Piscataway, NJ.

Manuscript received April 19, 2021; revised August 16, 2021.

apa pertahanan menggabungkan kerja komputer dan manusia dengan memperingatkan pengguna akhir tentang potensi pesan phishing, yang kemudian diselidiki lebih lanjut oleh pengguna akhir untuk menentukan apakah itu email phishing. Dan akhirnya, ada pertahanan manusia, di mana penerima email diandalkan untuk mengenali email sebagai berbahaya dan bertindak sesuai.

1) Deteksi dan Penghapusan Otomatis: Pendekatan deteksi dan penghapusan otomatis bertujuan untuk mengklasifikasikan email sebagai phishing atau sah dan memblokir atau menghapusnya sebelum pengguna akhir menemukannya. Upaya di bidang ini telah difokuskan pada peningkatan dan menemukan cara baru untuk mengidentifikasi pesan phishing yang masuk dan keluar menggunakan daftar hitam [10], heuristik [3, 13, 16, 23], dan pembelajaran mesin [9, 29]. Pendekatan ini menyaring email berdasarkan fitur yang diketahui yang secara konklusif mengidentifikasi email sebagai phishing. Namun, pendekatan otomatis mengandalkan algoritma probabilistik yang menghasilkan positif palsu, menyebabkan email sah diblokir atau dihapus. Selain itu, pendekatan otomatis memiliki kemampuan terbatas untuk mendeteksi variasi baru dari serangan phishing [12] dan tidak dapat mengidentifikasi semua email phishing yang lebih lama.

2) Peringatan Phishing: Peringatan phishing melengkapi teknik deteksi otomatis dengan memperingatkan pengguna akhir tentang potensi email phishing, alih-alih memblokir atau menghapusnya. Peringatan biasanya digunakan ketika deteksi otomatis tidak dapat secara konklusif mengklasifikasikan email sebagai phishing [25]. Dalam praktiknya, peringatan telah dilaporkan meningkatkan kemampuan pengguna akhir untuk mengidentifikasi email phishing [8, 26]. Upaya penelitian yang sedang berlangsung di area ini telah difokuskan pada menemukan cara yang lebih baik untuk merancang dan menyajikan peringatan kepada pengguna akhir.

Meskipun memiliki dampak positif, peringatan memiliki keterbatasan yang sama dengan pendekatan deteksi dan penghapusan otomatis. Mereka rentan terhadap positif palsu (menandai email sah sebagai berpotensi berbahaya) dan negatif palsu (membiarkan email berbahaya lolos tanpa peringatan, terutama serangan phishing zero-hour). Seperti yang dikemukakan oleh Yang et al., peringatan dan pelatihan pengguna harus saling melengkapi untuk meningkatkan efektivitasnya [37].

3) Pelatihan Pengguna: Peneliti dan praktisi keamanan telah mengembangkan berbagai metode dan materi untuk melatih pengguna mengidentifikasi dan bereaksi terhadap email phishing dengan tepat. Kumaraguru et al. [19] dan Caputo et al. [2] menemukan bahwa pelatihan tertanam (yaitu materi instruksional yang disajikan saat peserta mengklik URL dalam email phishing), yang sangat umum digunakan di organisasi besar, meningkatkan motivasi pengguna untuk belajar dan meningkatkan akuisisi pengetahuan. Rader et al. [27] menemukan bahwa orang juga belajar tentang penipuan phishing dan tindakan perlindungan dari cerita tentang insiden keamanan. Wash dan Cooper [35] menemukan bahwa pelatihan phishing tradisional yang berisi fakta dan saran bekerja lebih baik ketika disajikan oleh seorang ahli, sementara cerita keamanan naratif bekerja lebih baik ketika diceritakan oleh seorang rekan.

Pesan pelatihan phishing yang paling banyak dibagikan di seluruh pemerintah, bisnis, dan individu mengajarkan orang untuk mengidentifikasi tanda-tanda tertentu (misalnya alamat email pengirim, URL dalam email, tata bahasa atau ejaan yang buruk) atau menerapkan serangkaian aturan untuk mendeteksi, menghindari, dan melaporkan pesan phishing. Pesan pelatihan semacam itu telah dipelajari secara ekstensif dan menunjukkan potensi untuk meningkatkan ketahanan orang terhadap serangan phishing [4, 19]. Beberapa pesan berfokus pada perubahan perilaku, misalnya, tidak pernah mengklik URL atau membuka lampiran dalam email dari pengirim yang tidak dikenal.

Pesan pelatihan lainnya berfokus pada memberi tahu pengguna tentang jenis ancaman phishing yang umum dan cara mengidentifikasinya, dengan tujuan memanipulasi tingkat risiko dan selanjutnya tingkat ketakutan pada pengguna [5, 20]. Beberapa peneliti berpendapat bahwa ajakan ketakutan meningkatkan niat pengguna akhir untuk bertindak dengan aman. Namun, meskipun mampu mengubah niat perilaku pengguna akhir [5], ajakan ketakutan tidak memprediksi atau menghasilkan perilaku yang aman [6].

Pelatihan pengguna biasanya berfokus pada aspek pesan email dan mencoba mengubah cara orang berpikir tentang pesan email sehingga mereka memperhatikan fitur yang paling terkait dengan phishing. Studi telah menunjukkan bahwa ini meningkatkan pengetahuan pengguna, meningkatkan kemampuan mereka untuk mengidentifikasi email phishing, dan mengurangi jumlah serangan yang berhasil [2, 19, 35]. Namun, jumlah serangan phishing yang berhasil masih cukup tinggi, mencapai 32% dari semua pelanggaran perusahaan pada tahun 2018. Lebih banyak yang perlu dilakukan untuk meningkatkan kemampuan pengguna akhir dalam mengidentifikasi dan mencegah serangan phishing.

Sebagian besar pelatihan pengguna dikembangkan dari pemahaman tentang bagaimana dan mengapa orang jatuh ke dalam phishing [6]. Kami berhipotesis bahwa jika pelatihan lebih fokus pada aspek bagaimana orang sudah berpikir tentang dan menangani email secara umum, ini dapat membuka jalan baru untuk pelatihan phishing. Sayangnya, kami tidak memiliki pemahaman yang komprehensif tentang bagaimana pengguna non-ahli melakukannya. Masalah serupa dihadapi dalam pelatihan keterampilan teknis di mana peneliti menyelidiki cara untuk meningkatkan pelatihan pemecah masalah (teknisi) [15]. Mereka mempelajari dan mengidentifikasi proses konseptual umum dan strategi yang digunakan teknisi saat memecahkan masalah. Ini membantu mereka mengidentifikasi kesenjangan dalam metode dan pesan pelatihan yang ada dan selanjutnya membantu mereka mengidentifikasi area perbaikan. Kami berpendapat bahwa memahami proses dan strategi yang digunakan non-ahli untuk mengidentifikasi email phishing dapat mengungkapkan area potensial untuk perbaikan pelatihan phishing.

B. Bagaimana Orang Mengidentifikasi Email Phishing?

Downs et al. [7] menyelidiki strategi keputusan pengguna komputer non-ahli ketika menghadapi email yang mencurigakan. Mereka mengidentifikasi tiga strategi yang digunakan

peserta untuk memahami email yang mereka terima: 1) email ini tampaknya ditujukan untuk saya; 2) normal untuk mendengar dari perusahaan yang Anda lakukan bisnis dengannya dan 3) perusahaan terkemuka akan mengirim email. Downs et al. [7] menyatakan bahwa tidak ada strategi yang membantu orang mengidentifikasi pesan phishing yang dirancang dengan baik. Namun, studi tersebut melibatkan peran bermain dalam lingkungan yang terkendali. Kami tidak tahu strategi mana yang berlaku dan seberapa umum mereka dalam konteks alami dan kotak masuk orang.

Wash [34] melihat bagaimana ahli mengidentifikasi email phishing dengan mewawancarai 21 ahli IT tentang kejadian ketika mereka berhasil mengidentifikasi email sebagai phishing di kotak masuk mereka. Dia mengidentifikasi proses 3 tahap untuk mengidentifikasi email phishing. Pada tahap pertama, email diterima dan diperlakukan seperti email lainnya — konten dalam email diambil secara harfiah dan orang tersebut mencoba memahami email dan mencari tahu apa yang diminta untuk dilakukan. Saat mereka melakukan ini, mereka memperhatikan ketidaksesuaian — hal-hal yang ”terasa aneh” tentang email tersebut. Akhirnya, sesuatu memicu orang tersebut untuk berpikir bahwa email ini tidak sah — bahwa itu mungkin email phishing yang bukan seperti yang dikatakannya. Pada titik ini, mereka menjadi curiga dan mulai secara eksplisit mencari hal-hal yang dapat membantu mereka menentukan apakah email tersebut sah atau tidak. Potongan informasi baru ini sering memungkinkan mereka untuk secara konklusif mengidentifikasi email sebagai phishing.

Pekerjaan Wash [34] menunjukkan bagaimana beberapa pelajaran dari pelatihan phishing diterapkan dalam konteks dunia nyata. Namun, Wash hanya mempelajari para ahli. Para ahli mungkin memiliki keterampilan, pengalaman, dan pengetahuan yang lebih maju tentang phishing dan tindakan pencegahan dibandingkan dengan non-ahli. Kami tidak tahu temuan mana yang mungkin berlaku untuk non-ahli dan dapat digunakan untuk meningkatkan pelatihan mereka.

C. Phishing: Masalah Sosio-Teknis

Phishing adalah masalah sosio-teknis. Solusi otomatis tidak mendeteksi 100% email phishing. Oleh karena itu, pengguna akhir harus mengidentifikasi email ini di kotak masuk mereka. Seperti yang dikatakan oleh Khonji et al., tidak ada solusi tunggal yang ada untuk mengurangi serangan phishing [17]; sehingga teknik otomatis / peringatan dan pelatihan pengguna harus diterapkan untuk saling melengkapi [19]. Ini sebanding dengan Model Keju Swiss (SCM) James Reason [28] tentang penyebab dan respons kecelakaan. SCM adalah alat populer yang digunakan untuk menyelidiki atau menganalisis kompleksitas sistem dengan menunjukkan bahwa suatu insiden adalah hasil dari kombinasi kegagalan aktif oleh operator dan kondisi laten dari sistem. SCM menggambarkan sistem sosio-teknis sebagai beberapa irisan keju Swiss yang ditumpuk bersama, masing-masing irisan dengan lubang. Setiap irisan menggambarkan lapisan pertahanan sistem terhadap jenis kegagalan tertentu, sementara setiap lubang mewakili kegagalan dalam pertahanan sistem pada lapisan tertentu. Bryans dan Arief menerapkan model tersebut untuk memahami lapisan keamanan dan toleransi kesalahan dalam sistem komputer [1]. Mereka menggambarkan setiap lapisan sebagai mekanisme perlindungan terhadap jenis serangan tertentu, tetapi memiliki kelemahan (lubang) terhadap jenis lainnya.

Baik teknik deteksi dan penghapusan otomatis maupun peringatan mengandalkan pengguna akhir sebagai garis pertahanan terakhir terhadap phishing. Namun, jumlah serangan phishing yang berhasil baru-baru ini menunjukkan bahwa lebih banyak pekerjaan perlu dilakukan untuk meningkatkan pelatihan pengguna. Sementara sebagian besar pelatihan berfokus pada mengajarkan pengguna akhir untuk mengidentifikasi fitur yang diketahui dan konklusif dari email phishing, Downs et al. [7] dan Wash [34] menemukan bahwa pengguna akhir mengandalkan fitur selain pembeda konklusif untuk mengidentifikasi email phishing. Kita perlu mengeksplorasi cara-cara yang lebih baik untuk menjaga pengguna dalam lingkaran pertahanan terhadap serangan phishing. Lebih banyak penelitian perlu dilakukan untuk memahami bagaimana non-ahli mengidentifikasi email phishing, aspek atau informasi apa yang mereka andalkan, dan jenis hal yang mereka lakukan dalam proses tersebut. Pemahaman ini dapat membantu kita menyesuaikan dan menargetkan pelatihan phishing dan teknologi yang mendukung pengambilan keputusan manusia. Studi kami mengambil langkah pertama ke arah ini dengan menerapkan model Wash dalam survei untuk mempelajari teknik yang diikuti non-ahli untuk mengidentifikasi email phishing.

III. Methods and Sample

Dalam makalah ini, kami melihat bagaimana pengguna non-ahli mengidentifikasi email phishing, dan melihat apakah beberapa teknik yang diidentifikasi oleh Wash [34] pada ahli juga ada ketika non-ahli mengidentifikasi email phishing. Untuk mempelajari ini, kami melakukan survei di mana kami meminta pengguna internet non-ahli untuk mengingat email tertentu yang mereka terima yang ”mencurigakan atau berpotensi berbahaya,” dan kemudian menjawab pertanyaan tentang pengalaman mereka dengan email tersebut.

Kami mengajukan pertanyaan untuk mencoba memahami apa yang mereka perhatikan dan tidak perhatikan tentang email yang diterima responden dan memahami hal-hal apa yang tampaknya penting bagi mereka. Ini adalah catatan retrospektif tentang email masa lalu; kami mengharapkan bahwa responden tidak akan mengingat beberapa detail tentang apa yang terjadi. Kami membuat asumsi bahwa hal-hal yang tidak mereka ingat kemungkinan besar kurang penting dalam pemikiran mereka tentang email tersebut [18].

A. Survei

Kami memulai dengan instrumen survei yang secara longgar didasarkan pada Rader et al. [27]. Di awal survei, kami meminta responden untuk mengidentifikasi ”cerita” atau insiden tertentu di mana mereka menerima email yang mencurigakan atau berpotensi berbahaya. Kami kemudian meminta mereka untuk menjawab sejumlah pertanyaan tentang insiden tertentu tersebut.

Kami menyertakan pertanyaan penyaringan yang menanyakan kepada calon responden apakah mereka dapat mengingat menerima jenis email yang kami minati.

Survei memberi tahu responden bahwa ”Dalam survei ini, kami tertarik mendengar tentang email yang Anda terima yang mencurigakan atau berpotensi berbahaya dengan cara tertentu.” Kemudian meminta mereka untuk mengingat kembali email mereka, dan memberi tahu mereka bahwa tidak apa-apa untuk melihat kembali email mereka jika itu akan membantu. Kami bertanya ”Apakah Anda dapat mengingat pesan email yang mencurigakan atau berpotensi berbahaya yang pernah Anda terima?” Hanya responden yang menjawab ya untuk pertanyaan ini yang melanjutkan survei. 315 calon responden yang memenuhi syarat lainnya dikeluarkan dari penelitian karena mereka tidak menjawab ”Ya” untuk pertanyaan ini.

Seperti Rader et al. [27], kami memulai survei dengan proses elicitation untuk membuat responden mengidentifikasi satu ”email yang mencurigakan atau berpotensi berbahaya” untuk menjawab pertanyaan tentang. Elicitation ini mencakup tiga bagian. Pertama, kami meminta responden untuk menuliskan dalam kotak jawaban singkat ”cara-cara agar pesan email dapat tidak aman atau menyebabkan masalah keamanan” dan ”cara-cara yang Anda ketahui untuk mengenali email yang mencurigakan atau berpotensi berbahaya.” Prompt ini dimaksudkan untuk membantu memicu ingatan responden tentang email phishing potensial. Responden menulis rata-rata 12-14 kata untuk masing-masing prompt ini.

Kedua, kami meminta responden untuk ”memikirkan waktu di masa lalu ketika Anda secara pribadi menerima email yang mencurigakan atau berpotensi berbahaya” dan ”mencantumkan sebanyak mungkin email ini yang dapat Anda ingat” dalam kotak teks. Responden rata-rata menulis 15 kata sebagai tanggapan terhadap prompt ini.

Ketiga, kami menyajikan daftar ini kembali kepada responden dan meminta responden untuk ”Memilih satu pesan email dari daftar di atas yang mudah Anda ingat detailnya.” Kami meminta mereka untuk merangkum secara singkat email tertentu tersebut. Kami menyajikan ringkasan singkat ini kembali kepada responden di bagian atas setiap halaman survei berikutnya untuk membantu mereka mengingat email mana yang mereka jawab pertanyaan tentang. Ringkasan ini rata-rata sepanjang 21 kata.

Sisa survei meminta lebih banyak detail tentang insiden email tertentu yang dipilih oleh responden. Berdasarkan model Wash [34], kami mengidentifikasi enam proses yang digunakan para ahli dalam mendeteksi phishing. Kami menyusun pertanyaan di sekitar enam proses ini:

1) Memperhatikan: Hal-hal yang mereka perhatikan tentang email, seperti kapan mereka menerima email, jenis email (lampiran, dll.), konten kerja atau pribadi, akun kerja atau pribadi, dll.
2) Mengharapkan: Apa yang mereka harapkan dalam email; membangun dari memperhatikan dan membandingkan apa yang mereka perhatikan dengan apa yang mereka harapkan. Apakah mereka pernah menerima email lain seperti ini, berinteraksi dengan pengirim sebelumnya, apakah email tersebut diharapkan, dll.
3) Mencurigai: Apa yang terasa ”aneh” tentang email — subjek, dari, isi, dll. Apa yang ada dalam email yang membuat mereka curiga terhadap email tersebut. Apakah itu berisi tautan, lampiran, dll.
4) Menyelidiki: Apa yang mereka cari secara eksplisit setelah mereka mencurigai email tersebut (jika ada) untuk mengetahui apakah email tersebut sah atau penipuan. Hal-hal seperti ”apakah Anda melihat header, atau mengarahkan kursor ke tautan, atau mencoba menghubungi pengirim?”
5) Memutuskan: Bagaimana keputusan sah/phish dibuat. Apakah Anda memutuskan, dan jika ya, bagaimana? Seberapa yakin Anda?
6) Bertindak: Setelah memutuskan, apa yang Anda lakukan dengan email tersebut? Melaporkannya? Hanya menghapusnya? Bagaimana perasaan Anda tentang email tersebut? Takut? Kecemasan? Kegelisahan?

Instrumen survei lengkap dapat ditemukan dalam materi tambahan.

B. Sampel

Kami bekerja sama dengan Qualtrics untuk menyebarkan survei kami kepada panel peserta di AS pada Februari 2020, yang tepat sebelum pandemi COVID. Kami mengecualikan responden yang memiliki keahlian teknis atau bekerja sebagai profesional teknologi karena kami secara khusus menginginkan responden non-ahli. Kami menetapkan kuota pada usia, jenis kelamin, dan etnis yang kira-kira sesuai dengan populasi AS, untuk mencoba mendapatkan sampel yang lebih representatif. Kami menerima total 297 tanggapan yang valid. Responden diberi kompensasi oleh Qualtrics dengan poin yang dapat ditukarkan dengan barang.

Tabel 1 merangkum demografi sampel kami. Sampel kami mencapai kuota dan oleh karena itu kira-kira sesuai dengan populasi AS dalam hal tersebut. Itu juga kebetulan mendekati populasi AS dalam hal pendidikan.

Hanya sekitar 50% dari sampel kami yang saat ini bekerja penuh waktu atau paruh waktu. Ini lebih rendah daripada populasi AS (yang sekitar 61% bekerja pada saat survei [24]). Ini adalah cara utama kami percaya sampel kami berbeda dari populasi AS yang lebih besar. Kami tidak yakin bagaimana ini mungkin mempengaruhi tanggapan tentang email phishing.

Mayoritas responden dalam sampel kami memiliki pengalaman sebelumnya dengan insiden keamanan siber; hanya 17% responden yang menunjukkan bahwa mereka belum pernah menjadi korban insiden keamanan siber. Sekitar setengah dari sampel melaporkan memiliki virus (52%), dan hampir setengahnya melaporkan menerima pemberitahuan tentang pelanggaran data (47%). Sekitar seperempat (26%) telah menjadi korban penipuan kartu kredit, dan 6% melaporkan menjadi korban pencurian identitas yang lebih serius daripada penipuan kartu kredit. 18% melaporkan memiliki perangkat yang diretas. Menariknya, 16% responden melaporkan pernah tertipu oleh email phishing atau email scam lainnya. Statistik ini menunjukkan bahwa sampel kami juga agak bias terhadap orang-orang yang memiliki pengalaman sebelumnya dengan insiden keamanan siber.

TABLE I
DEMOGRAFI SAMPEL SURVEI. KAMI MENERIMA TANGGAPAN YANG VALID DARI TOTAL 297 RESPONDEN. KUOTA DIGUNAKAN PADA USIA, JENIS KELAMIN, DAN ETNIS UNTUK KIRA-KIRA MENCOCOKKAN DEMOGRAFI AMERIKA SERIKAT.

Kategori	Subkategori	N	%
Usia	18–30	75	25%
	30–50	104	35%
	50–65	73	25%
	Lebih dari 65	45	15%
Jenis Kelamin	Pria	151	49%
	Wanita	156	50%
	Lainnya	2	1%
	Lebih memilih untuk tidak menjawab	1	0%
Etnis	Putih	202	64%
	Hispanik, Latino, atau Spanyol	51	16%
	Hitam atau Afrika Amerika	37	12%
	Asia	18	6%
	Indian Amerika atau Penduduk Asli Alaska	8	3%
Pendidikan	Tidak ada Perguruan Tinggi	71	24%
	Teknik, Perdagangan, atau Kejuruan	22	7%
	Beberapa perguruan tinggi	102	34%
	Gelar Perguruan Tinggi	102	34%
Pekerjaan	Bekerja Penuh Waktu	105	35%
	Bekerja Paruh Waktu	42	14%
	Pengangguran dan mencari pekerjaan	24	8%
	Pengangguran dan tidak mencari	25	8%
	Pensiunan	45	19%
	Cacat	29	10%
	Pelajar	16	5%
Pendapatan Rumah Tangga Tahunan (USD)	Kurang dari $25,000	66	22%
	$25,000 hingga $34,999	51	17%
	$35,000 hingga $49,999	35	12%
	$50,000 hingga $74,999	69	23%
	$75,000 hingga $99,999	33	11%
	$100,000 hingga $149,999	30	10%
	$150,000 hingga $199,999	7	2%
	$200,000 atau lebih	6	2%

C. Analisis

Di akhir survei, kami meminta responden untuk ”tolong tuliskan cerita email tersebut seolah-olah Anda menceritakannya kepada seorang teman.” Kami menyediakan kotak teks besar untuk peserta memasukkan cerita, dan mengharuskan responden memasukkan setidaknya 300 karakter ke dalam kotak ini. Responden rata-rata lebih dari 400 karakter (rata-rata=411, min=300, maks=1523), yang sekitar 80 kata per cerita rata-rata (rata-rata=81, min=41, maks=288). Kami memiliki dua asisten peneliti yang mengkodekan cerita ini secara paralel, bertemu setiap minggu untuk memperbarui buku kode, mengukur kesepakatan, dan menyelesaikan perbedaan. Kami akhirnya memiliki buku kode yang mengkodekan cerita untuk fitur-fitur yang diatur dalam 5 kategori: properti pengirim email yang diklaim; tindakan yang diminta oleh email; apa yang terasa aneh dalam email; tindakan yang diambil dalam cerita; dan keputusan akhir tentang email.

Setelah pelatihan dan pengembangan buku kode, kedua pengkode mengkodekan semua 297 cerita secara independen untuk buku kode 39 kode yang berbeda. Setelah pengkodean awal ini, lebih dari setengah kode memiliki alpha Cronbach di atas 0,7, dan hanya 3 kode yang memiliki alpha di bawah 0,5. Kami menghapus 3 kode dengan kesepakatan rendah. Kedua pengkode kemudian bertemu dan membicarakan semua contoh di mana ada ketidaksepakatan dan secara bersama-sama menyetujui keputusan akhir tentang semua kode untuk semua cerita.

Dalam makalah ini, hasil dari pengkodean manual ini akan secara eksplisit diberi label sebagai hasil dari pengkodean manual. Setiap hasil yang tidak diberi label sebagai hasil dari pengkodean manual adalah data laporan diri langsung dari pertanyaan dalam tubuh utama survei. 13 (4%) dari cerita disepakati sebagai ”bukan cerita” oleh kedua pengkode. Ini adalah contoh di mana peserta mengisi kotak teks ini untuk seluruh survei, tetapi tidak menggambarkan pengalaman dengan email tertentu, dan sebaliknya menggambarkan pengalaman yang lebih umum. Tanggapan ini tidak termasuk dalam statistik untuk pengkodean manual.

Materi replikasi untuk analisis ini tersedia di https://osf.io/82sd9/. Selain itu, semua cerita disajikan persis seperti yang dimasukkan oleh responden, termasuk kesalahan ketik.

IV. FINDINGS

Dalam survei ini, kami meminta responden untuk mengidentifikasi ”pesan email yang mencurigakan atau berpotensi berbahaya yang Anda terima di masa lalu.” 315 responden yang memenuhi syarat tidak dapat mengidentifikasi email, dan 311 responden yang memenuhi syarat dapat melakukannya. Kuota hanya diterapkan pada responden yang memenuhi syarat yang mengingat email tersebut, dan responden diberi insentif untuk mengingat email tersebut agar dapat berpartisipasi dalam survei dan menerima pembayaran insentif. Tujuan kami bukan untuk menemukan seberapa umum phishing di antara kelompok demografis yang berbeda, dan sampel ini tidak boleh diartikan sebagai pengukuran prevalensi phishing. Namun, ini

menunjukkan bahwa sekitar 50% dari orang-orang non-ahli dalam pool subjek Qualtrics memiliki cerita tentang email phishing tertentu yang mereka terima, yang menunjukkan betapa luasnya pengalaman dengan email-email ini.

Hampir semua pertanyaan yang tersisa dalam survei kemudian meminta responden untuk memberikan lebih banyak detail tentang insiden spesifik di mana mereka menerima email yang mereka pilih untuk diceritakan kepada kami: apa yang terjadi saat mereka menerimanya, apa yang mereka perhatikan, dan bagaimana mereka menanganinya? Dalam sebagian besar makalah ini, kami melaporkan statistik tentang tanggapan terhadap pertanyaan pilihan ganda.

Berdasarkan temuan dari Wash [34], kami mengorganisir survei berdasarkan enam aktivitas berbeda yang perlu dilakukan seseorang untuk mengenali email phishing: 1) Memperhatikan aspek-aspek email; 2) Membentuk ekspektasi tentang apa yang seharusnya dan tidak seharusnya ada dalam email; 3) Menjadi curiga terhadap email; 4) Menyelidiki email; 5) Memutuskan apakah email mencurigakan atau tidak; dan 6) Bertindak berdasarkan keputusan tersebut.

Enam aktivitas ini memberikan cara bagi kami untuk menggambarkan apa yang umumnya terjadi ketika seseorang menerima email phishing, dan untuk melihat pola dalam apa yang mereka perhatikan dan apa yang mereka lakukan. Kami mengorganisir deskripsi temuan kami dalam makalah ini di sekitar enam aktivitas berbeda ini.

1) Insiden: Setiap peserta diminta untuk menjawab pertanyaan tentang satu insiden yang mereka alami. Kami mulai dengan menggambarkan jenis insiden yang dilaporkan oleh responden. Setiap insiden adalah email yang diterima peserta dan dianggap mencurigakan atau berpotensi berbahaya. Semua insiden ini mewakili email yang berhasil melewati pertahanan teknis dan masuk ke kotak masuk peserta, sehingga tidak termasuk email phishing yang berhasil difilter oleh perlindungan phishing teknis. Namun, email-email ini tidak seragam; responden melaporkan menerima berbagai jenis email phishing yang berbeda.

Kami meminta setiap responden untuk mengidentifikasi daftar kemungkinan insiden/email yang memenuhi syarat, dan kemudian meminta mereka untuk memilih satu yang ”mudah diingat detailnya” dan kemudian menjawab lebih banyak pertanyaan tentang yang satu itu. Kami memiliki total lima pertanyaan yang mencoba memahami secara luas tentang apa email-email ini — satu pertanyaan di awal yang meminta responden untuk merangkum insiden, satu pertanyaan di akhir yang meminta responden untuk menjelaskan seluruh insiden, dan kemudian tiga pertanyaan yang meminta deskripsi singkat, 5-kata tentang insiden yang dipilih. Di sini kami menggunakan deskripsi 5-kata ini untuk menggambarkan jenis insiden yang dilaporkan orang.

Ketika diminta untuk merangkum insiden di awal survei, responden merespons dengan rata-rata 21 kata (median: 17 kata). Dalam ringkasan ini, responden sebagian besar melaporkan fakta tentang email yang mereka terima, dengan kata-kata yang paling umum adalah email (39% responden), akun (17%), uang (15%), tautan (13%) dan menerima (11%).

Selain ringkasan, kami meminta responden, ”Dalam sekitar lima kata” untuk menggambarkan apa yang membuat email mencurigakan, apa yang membuat email sulit untuk dipahami, dan apa yang diminta email tersebut untuk mereka lakukan. Responden melaporkan bahwa mereka curiga terutama melihat alamat email/pengirim atau karena melibatkan uang. Email-email tersebut sebagian besar meminta responden untuk mengklik tautan (22%), untuk uang (17%), atau untuk ”informasi” (14%). Bersama-sama, ringkasan ini menunjukkan bahwa sebagian besar cerita phishing adalah tentang masalah ekonomi (uang) atau meminta atau memberikan informasi.

Sekitar 81% responden menunjukkan bahwa mereka merasa mudah mengingat email semacam itu. Email-email yang dipilih responden untuk dijawab tersebar luas dalam waktu: 24% responden menerimanya dalam minggu terakhir; 30% dalam bulan terakhir (tetapi bukan minggu terakhir); 25% dalam tahun terakhir (tetapi bukan bulan terakhir); dan 15% lebih dari setahun yang lalu. Dalam pengkodean manual, kami mengkodekan cerita insiden lengkap untuk informasi tentang siapa pengirim email yang diklaim. Ini bukan siapa yang sebenarnya mengirim email, tetapi siapa yang berpura-pura menjadi pengirim email. 44% menunjukkan bahwa email tersebut berasal dari kelompok atau organisasi, dan 25% menunjukkan bahwa email tersebut tampaknya berasal dari individu. Dalam 30% cerita, peserta menunjukkan bahwa mereka memiliki hubungan sebelumnya dengan pengirim yang diklaim, dan 14% cerita peserta secara eksplisit menyatakan bahwa mereka tidak memiliki hubungan sebelumnya. 76% dari hubungan sebelumnya adalah dengan kelompok atau organisasi; menunjukkan bahwa email yang berpura-pura berasal dari organisasi lebih mungkin dilihat sebagai bagian dari hubungan sebelumnya.

Sebagai contoh cerita tentang email dari organisasi yang peserta memiliki hubungan sebelumnya, pertimbangkan cerita berikut tentang email dari Amazon.com:

Cerita P233: *menerima email yang tampaknya berasal dari amazon. Email tersebut memiliki nama dan alamat saya tetapi mengatakan saya berutang uang untuk pembelian. Saya tidak membeli apa pun untuk sementara waktu sehingga itu tampak aneh. Email tersebut memiliki kesalahan ejaan dan tautan yang aneh. Saya melihat email tersebut dengan cermat, kemudian memeriksa akun amazon saya di situs web mereka. Tidak ada apa pun di sana tentang pesanan atau utang uang.*

Pengirim sebenarnya bervariasi secara luas di seluruh cerita: sekitar 12% mengatakan itu adalah bank atau lembaga keuangan, 8% mengatakan email tersebut tampaknya berasal dari orang asing, 4% dari pemerintah, dan 2% dari organisasi dukungan IT.

Dalam pengkodean manual cerita, kami juga mengkodekan untuk jenis informasi apa yang diminta. 30% cerita menyebutkan bahwa penerima email akan menerima semacam barang berharga (uang, hadiah, tawaran pekerjaan, dll.), dan 19% cerita melaporkan bahwa email meminta penerima untuk mengirim uang. 19% cerita menyebutkan bahwa email meminta informasi pribadi, 10% cerita meminta informasi teknis seperti nama pengguna atau kata sandi, dan 10% cerita meminta informasi keuangan seperti nomor rekening bank, nomor kartu kredit, dll. Ini menunjukkan bahwa responden kami menerima email dengan berbagai permintaan, tanpa jenis permintaan tertentu yang sangat umum. Apa yang dianggap pengguna

akhir sebagai phishing sangat beragam, dan pelatihan yang berfokus terutama pada petunjuk mungkin melewatkan kelas pesan email yang menonjol bagi pengguna akhir sebagai berpotensi berbahaya.

A. Memperhatikan

1) Apa yang diperhatikan orang dalam email: Saat seseorang membaca email, mereka tidak dapat memperhatikan dan mengingat semua tentang email tersebut. Sebaliknya, hal-hal dalam email yang paling mudah mereka pahami dan hubungkan adalah yang paling mudah diperhatikan dan diingat [18]. Kami bertanya kepada responden "Aspek apa dari email yang menonjol bagi Anda?" dan memungkinkan mereka untuk mencentang semua yang berlaku. Jawaban atas pertanyaan ini menunjukkan kepada kami, untuk email-email phishing yang dicurigai ini, aspek apa dari email yang paling penting bagi responden, karena mereka adalah yang paling mudah diingat.

Jauh lebih banyak, aspek yang diperhatikan oleh jumlah orang terbesar adalah bahwa email tersebut mencakup permintaan untuk tindakan. 76% responden memperhatikan ini tentang email tersebut. Ini sesuai dengan penelitian sebelumnya yang menunjukkan bahwa orang cenderung menggunakan email sebagai daftar tugas [36]; mereka dengan cepat fokus pada apa yang diminta email untuk mereka lakukan. Ini juga sesuai dengan temuan Wash [34] bahwa permintaan untuk tindakan (tautan tindakan) adalah pemicu penting bagi para ahli.

Aspek kedua yang paling umum diperhatikan dari email adalah tentang apa email tersebut, dengan 52% responden memperhatikan ini. Topik email, dan apakah topik tersebut relevan dengan penerima email, umumnya dianggap sebagai aspek penting dari phishing. Data ini mendukung gagasan tersebut, dan menunjukkan bahwa ini adalah sesuatu yang dengan cepat dapat diidentifikasi dan diingat oleh orang-orang tentang email.

Banyak pekerjaan sebelumnya tentang phishing telah berfokus pada "pembeda konklusif": aspek-aspek email yang dapat membantu penerima untuk secara konklusif membedakan email yang sah dari email phishing, atau setidaknya sangat menunjukkan phishing. Misalnya, pelatihan phishing biasanya berfokus pada aspek seperti URL yang tidak sesuai dalam tautan, urgensi dalam permintaan tindakan, atau tata bahasa/ejaan yang buruk. Namun, Wash menekankan bahwa ketika para ahli mengidentifikasi email phishing di kotak masuk mereka sendiri, mereka malah mencari ketidaksesuaian yang lebih kecil, yaitu hal-hal yang tampak aneh tentang email tersebut, tetapi tidak selalu menunjukkan phishing dan tentu saja tidak cukup untuk secara konklusif mengidentifikasi phishing.

Dua hal pertama yang diperhatikan responden — permintaan untuk tindakan dan topik email — tidak secara konklusif menunjukkan bahwa email tersebut adalah pesan phishing, dan biasanya bukan bagian dari pelatihan phishing. Sebaliknya, mereka hanya menunjukkan bahwa ada sesuatu yang aneh tentang email tersebut. Namun, bagi beberapa orang, itu mungkin sudah cukup. Misalnya, pertimbangkan cerita ini:

Cerita P19: *Saya mendapat email Jumat lalu dari salah satu perusahaan yang kami bekerja untuk mereka yang membayar kami untuk menyediakan layanan bagi mereka dan saya segera bisa tahu itu adalah email palsu karena perusahaan yang menyamar sebagai pengirim email adalah perusahaan yang membayar kami, kami tidak membayar mereka. Saya menelepon perusahaan yang kami bekerja untuk dan melaporkannya kepada mereka sehingga mereka tahu seseorang mencoba menyamar sebagai mereka.*

Dua aspek email berikutnya yang paling umum diperhatikan lebih sering dikaitkan dengan identifikasi phishing: tautan dalam email (44%), kesalahan atau kualitas buruk (41%). Ini sering ditemukan dalam email phishing (terutama jenis email phishing yang mungkin dapat dideteksi oleh non-ahli dalam sampel kami).

Sekitar 38% responden melaporkan bahwa nama pengirim menonjol bagi mereka. Aspek email lainnya, seperti lampiran, gambar, format, atau panjang email, diperhatikan oleh kurang dari 20% responden, meskipun semuanya penting bagi sebagian kecil pengguna. Temuan ini menunjukkan bahwa orang tampaknya secara alami memperhatikan tindakan dan topik email jauh lebih banyak daripada mereka memperhatikan pembeda konklusif seperti URL atau kesalahan ketik. Ini penting, karena seseorang tidak dapat menggunakan fitur untuk mendeteksi phishing kecuali mereka pertama kali memperhatikan fitur tersebut.

V. The Design, Intent, and Limitations of the Templates

The templates are intended to **approximate the final look and page length of the articles/papers**. **They are NOT intended to be the final produced work that is displayed in print or on IEEEXplore®**. They will help to give the authors an approximation of the number of pages that will be in the final version. The structure of the LaTeX files, as designed, enable easy conversion to XML for the composition systems used by the IEEE. The XML files are used to produce the final print/IEEEXplore pdf and then converted to HTML for IEEEXplore.

VI. Where to Get LaTeX Help — User Groups

The following online groups are helpful to beginning and experienced LaTeX users. A search through their archives can provide many answers to common questions.

http://www.latex-community.org/
https://tex.stackexchange.com/

VII. Other Resources

See [10]–[14] for resources on formatting math into text and additional help in working with LaTeX.

VIII. Text

For some of the remainer of this sample we will use dummy text to fill out paragraphs rather than use live text that may violate a copyright.

Itam, que ipiti sum dem velit la sum et dionet quatibus apitet voloritet audam, qui aliciant voloreicid quaspe volorem

ut maximusandit faccum conemporerum aut ellatur, nobis arcimus. Fugit odi ut pliquia incitium latum que cusapere perit molupta eaquaeria quod ut optatem poreiur? Quiaerr ovitior suntiant litio bearciur?

Onseque sequaes rectur autate minullore nusae nestiberum, sum voluptatio. Et ratem sequiam quaspername nos rem repudandae volum consequis nos eium aut as molupta tectum ulparumquam ut maximillesti consequas quas inctia cum volectinusa porrum unt eius cusaest exeritatur? Nias es enist fugit pa vollum reium essusam nist et pa aceaqui quo elibusdandis deligendus que nullaci lloreri bla que sa coreriam explacc atiumquos simolorpore, non prehendunt lam que occum [15] si aut aut maximus eliaeruntia dia sequiamenime natem sendae ipidemp orehend uciisi omnienetus most verum, ommolendi omnimus, est, veni aut ipsa volendelist mo conserum volores estisciis recessi nveles ut poressitatur sitiis ex endi diti volum dolupta aut aut odi as eatquo cullabo remquis toreptum et des accus dolende pores sequas dolores tinust quas expel moditae ne sum quiatis nis endipie nihilis etum fugiae audi dia quiasit quibus. Ibus el et quatemo luptatque doluptaest et pe volent rem ipidusa eribus utem venimolorae dera qui acea quam etur aceruptat. Gias anis doluptaspic tem et aliquis alique inctiuntiur?

Sedigent, si aligend elibuscid ut et ium volo tem eictore pellore ritatus ut ut ullatus in con con pere nos ab ium di tem aliqui od magnit repta volectur suntio. Nam isquiante doluptis essit, ut eos suntionsecto debitiur sum ea ipitiis adipit, oditiore, a dolorerempos aut harum ius, atquat.

Rum rem ditinti sciendunti volupiciendi sequiae nonsect oreniatur, volores sition ressimil inus solut ea volum harumqui to see(1) mint aut quat eos explis ad quodi debis deliqui aspel earcius.

$$x = \sum_{i=0}^{n} 2iQ. \tag{1}$$

Alis nime volorempera perferi sitio denim repudae pre ducilit atatet volecte ssimillorae dolore, ut pel ipsa nonsequiam in re nus maiost et que dolor sunt eturita tibusanis eatent a aut et dio blaudit reptibu scipitem liquia consequodi od unto ipsae. Et enitia vel et experferum quiat harum sa net faccae dolut voloria nem. Bus ut labo. Ita eum repraer rovitia samendit aut et volupta tecupti busant omni quiae porro que nossimodic temquis anto blacita conse nis am, que ereperum eumquam quaescil imenisci quae magnimos recus ilibeaque cum etum iliate prae parumquatemo blaceaquiam quundia dit apienditem rerit re eici quaes eos sinvers pelecabo. Namendignis as exerupit aut magnim ium illabor roratecte plic tem res apiscipsam et vernat untur a deliquaest que non cus eat ea dolupiducim fugiam volum hil ius dolo eaquis sitis aut landesto quo corerest et auditaquas ditae voloribus, qui optaspis exero cusa am, ut plibus.

IX. Some Common Elements

A. Sections and Subsections

Enumeration of section headings is desirable, but not required. When numbered, please be consistent throughout the article, that is, all headings and all levels of section headings in the article should be enumerated. Primary headings are designated with Roman numerals, secondary with capital letters, tertiary with Arabic numbers; and quaternary with lowercase letters. Reference and Acknowledgment headings are unlike all other section headings in text. They are never enumerated. They are simply primary headings without labels, regardless of whether the other headings in the article are enumerated.

Fig. 1. Simulation results for the network.

B. Citations to the Bibliography

The coding for the citations is made with the LaTeX `\cite` command. This will display as: see [10].

For multiple citations code as follows: `\cite{ref1,ref2,ref3}` which will produce [10]–[12]. For reference ranges that are not consecutive code as `\cite{ref1,ref2,ref3,ref9}` which will produce [10]–[12], [18]

C. Lists

In this section, we will consider three types of lists: simple unnumbered, numbered, and bulleted. There have been many options added to IEEEtran to enhance the creation of lists. If your lists are more complex than those shown below, please refer to the original "IEEEtran_HOWTO.pdf" for additional options.

A plain unnumbered list:

bare_jrnl.tex
bare_conf.tex
bare_jrnl_compsoc.tex
bare_conf_compsoc.tex
bare_jrnl_comsoc.tex

A simple numbered list:

1) bare_jrnl.tex
2) bare_conf.tex
3) bare_jrnl_compsoc.tex
4) bare_conf_compsoc.tex
5) bare_jrnl_comsoc.tex

A simple bulleted list:

- bare_jrnl.tex
- bare_conf.tex
- bare_jrnl_compsoc.tex
- bare_conf_compsoc.tex
- bare_jrnl_comsoc.tex

D. Figures

Fig. 1 is an example of a floating figure using the graphicx package. Note that `\label` must occur AFTER (or within) `\caption`. For figures, `\caption` should occur after the `\includegraphics`.

Fig. 2(a) and 2(b) is an example of a double column floating figure using two subfigures. (The subfig.sty package must be loaded for this to work.) The subfigure `\label` commands

(a) (b)

Fig. 2. Dae. Ad quatur autat ut porepel itemoles dolor autem fuga. Bus quia con nessunti as remo di quatus non perum que nimus. (a) Case I. (b) Case II.

TABLE II
AN EXAMPLE OF A TABLE

One	Two
Three	Four

are set within each subfloat command, and the \label for the overall figure must come after \caption. \hfil is used as a separator to get equal spacing. The combined width of all the parts of the figure should do not exceed the text width or a line break will occur.

Note that often IEEE papers with multi-part figures do not place the labels within the image itself (using the optional argument to \subfloat[]), but instead will reference/describe all of them (a), (b), etc., within the main caption. Be aware that for subfig.sty to generate the (a), (b), etc., subfigure labels, the optional argument to \subfloat must be present. If a subcaption is not desired, leave its contents blank, e.g.,\subfloat[].

X. TABLES

Note that, for IEEE-style tables, the \caption command should come BEFORE the table. Table captions use title case. Articles (a, an, the), coordinating conjunctions (and, but, for, or, nor), and most short prepositions are lowercase unless they are the first or last word. Table text will default to \footnotesize as the IEEE normally uses this smaller font for tables. The \label must come after \caption as always.

XI. ALGORITHMS

Algorithms should be numbered and include a short title. They are set off from the text with rules above and below the title and after the last line.

[H] Weighted Tanimoto ELM. TRAIN($\mathbf{XT}$) **select randomly** $W \subset \mathbf{X}$ $N_{\mathbf{t}} \leftarrow |\{i : \mathbf{t}_i = \mathbf{t}\}|$ **for** $\mathbf{t} = -1, +1$ $B_i \leftarrow \sqrt{\text{MAX}(N_{-1}, N_{+1})/N_{\mathbf{t}_i}}$ **for** $i = 1, ..., N$ $\hat{\mathbf{H}} \leftarrow B \cdot (\mathbf{X}^T\mathbf{W})/(⊮\mathbf{X} + ⊮\mathbf{W} - \mathbf{X}^T\mathbf{W})$ $\beta \leftarrow \left(I/C + \hat{\mathbf{H}}^T\hat{\mathbf{H}}\right)^{-1}(\hat{\mathbf{H}}^T B \cdot \mathbf{T})$ **return** $\mathbf{W}, \beta$ /[11] PREDICT($\mathbf{X}$) $\mathbf{H} \leftarrow (\mathbf{X}^T\mathbf{W})/(⊮\mathbf{X} + ⊮\mathbf{W} - \mathbf{X}^T\mathbf{W})$ **return** SIGN($\mathbf{H}\beta$)

Que sunt eum lam eos si dic to estist, culluptium quid qui nestrum nobis reiumquiatur minimus minctem. Ro moluptat fuga. Itatquiam ut laborpo rersped exceres vollandi repudaerem. Ulparci sunt, qui doluptaquis sumquia ndestiu sapient iorepella sunti veribus. Ro moluptat fuga. Itatquiam ut laborpo rersped exceres vollandi repudaerem.

XII. MATHEMATICAL TYPOGRAPHY AND WHY IT MATTERS

Typographical conventions for mathematical formulas have been developed to **provide uniformity and clarity of presentation across mathematical texts**. This enables the readers of those texts to both understand the author's ideas and to grasp new concepts quickly. While software such as LaTeX and MathType® can produce aesthetically pleasing math when used properly, it is also very easy to misuse the software, potentially resulting in incorrect math display.

IEEE aims to provide authors with the proper guidance on mathematical typesetting style and assist them in writing the best possible article. As such, IEEE has assembled a set of examples of good and bad mathematical typesetting [10]–[14].

Further examples can be found at http://journals.ieeeauthorcenter.ieee.org/wp-content/uploads/sites/7/IEEE-Math-Typesetting-Guide-for-LaTeX-Users.pdf

A. Display Equations

The simple display equation example shown below uses the "equation" environment. To number the equations, use the \label macro to create an identifier for the equation. LaTeX will automatically number the equation for you.

$$x = \sum_{i=0}^{n} 2iQ. \tag{2}$$

is coded as follows:

```
\begin{equation}
\label{deqn_ex1}
x = \sum_{i=0}^{n} 2{i} Q.
\end{equation}
```

To reference this equation in the text use the \ref macro. Please see (2)
is coded as follows:

```
Please see (\ref{deqn_ex1})
```

B. Equation Numbering

Consecutive Numbering: Equations within an article are numbered consecutively from the beginning of the article to the end, i.e., (1), (2), (3), (4), (5), etc. Do not use roman numerals or section numbers for equation numbering.

Appendix Equations: The continuation of consecutively numbered equations is best in the Appendix, but numbering as (A1), (A2), etc., is permissible.

Hyphens and Periods: Hyphens and periods should not be used in equation numbers, i.e., use (1a) rather than (1-a) and (2a) rather than (2.a) for subequations. This should be consistent throughout the article.

C. Multi-Line Equations and Alignment

Here we show several examples of multi-line equations and proper alignments.

A single equation that must break over multiple lines due to length with no specific alignment.

$$\begin{multline}\text{The first line of this example}\\ \text{The second line of this example}\\ \text{The third line of this example}\end{multline} \tag{3}$$

is coded as:

```
\begin{multline}
\text{The first line of this example}\\
\text{The second line of this example}\\
\text{The third line of this example}
\end{multline}
```

A single equation with multiple lines aligned at the = signs

$$a = c + d \tag{4}$$
$$b = e + f \tag{5}$$

is coded as:

```
\begin{align}
a &= c+d \\
b &= e+f
\end{align}
```

The `align` environment can align on multiple points as shown in the following example:

$$x = y \qquad X = Y \qquad a = bc \tag{6}$$
$$x' = y' \qquad X' = Y' \qquad a' = bz \tag{7}$$

is coded as:

```
\begin{align}
x &= y & X &=Y & a &=bc\\
x' &= y' & X' &=Y' &a' &=bz
\end{align}
```

D. Subnumbering

The amsmath package provides a `subequations` environment to facilitate subnumbering. An example:

$$f = g \tag{8a}$$
$$f' = g' \tag{8b}$$
$$\mathcal{L}f = \mathcal{L}g \tag{8c}$$

is coded as:

```
\begin{subequations}\label{eq:2}
\begin{align}
f&=g \label{eq:2A}\\
f' &=g' \label{eq:2B}\\
\mathcal{L}f &= \mathcal{L}g \label{eq:2c}
\end{align}
\end{subequations}
```

E. Matrices

There are several useful matrix environments that can save you some keystrokes. See the example coding below and the output.

A simple matrix:

$$\begin{matrix} 0 & 1 \\ 1 & 0 \end{matrix} \tag{9}$$

is coded as:

```
\begin{equation}
\begin{matrix}  0 &  1 \\
1 &  0 \end{matrix}
\end{equation}
```

A matrix with parenthesis

$$\begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \tag{10}$$

is coded as:

```
\begin{equation}
\begin{pmatrix} 0 & -i \\
 i &  0 \end{pmatrix}
\end{equation}
```

A matrix with square brackets

$$\begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \tag{11}$$

is coded as:

```
\begin{equation}
\begin{bmatrix} 0 & -1 \\
1 &  0 \end{bmatrix}
\end{equation}
```

A matrix with curly braces

$$\begin{Bmatrix} 1 & 0 \\ 0 & -1 \end{Bmatrix} \tag{12}$$

is coded as:

```
\begin{equation}
\begin{Bmatrix} 1 &  0 \\
0 & -1 \end{Bmatrix}
\end{equation}
```

A matrix with single verticals

$$\begin{vmatrix} a & b \\ c & d \end{vmatrix} \tag{13}$$

is coded as:

```
\begin{equation}
\begin{vmatrix} a &  b \\
c &  d \end{vmatrix}
\end{equation}
```

A matrix with double verticals

$$\begin{Vmatrix} i & 0 \\ 0 & -i \end{Vmatrix} \tag{14}$$

is coded as:

```
\begin{equation}
\begin{Vmatrix} i &  0 \\
0 & -i \end{Vmatrix}
\end{equation}
```

F. Arrays

The `array` environment allows you some options for matrix-like equations. You will have to manually key the fences, but there are other options for alignment of the columns and for setting horizontal and vertical rules. The argument to `array` controls alignment and placement of vertical rules.

A simple array

$$\left(\begin{array}{cccc} a+b+c & uv & x-y & 27 \\ a+b & u+v & z & 134 \end{array} \right) \tag{15}$$

is coded as:

```
\begin{equation}
\left(
\begin{array}{cccc}
a+b+c & uv & x-y & 27\\
a+b & u+v & z & 134
\end{array} \right)
\end{equation}
```

A slight variation on this to better align the numbers in the last column

$$\left(\begin{array}{cccc} a+b+c & uv & x-y & 27 \\ a+b & u+v & z & 134 \end{array} \right) \tag{16}$$

is coded as:

```
\begin{equation}
\left(
\begin{array}{cccr}
a+b+c & uv & x-y & 27\\
a+b & u+v & z & 134
\end{array} \right)
\end{equation}
```

An array with vertical and horizontal rules

$$\left(\begin{array}{c|c|c|r} a+b+c & uv & x-y & 27 \\ \hline a+b & u+v & z & 134 \end{array} \right) \tag{17}$$

is coded as:

```
\begin{equation}
\left(
\begin{array}{c|c|c|r}
a+b+c & uv & x-y & 27\\
a+b & u+v & z & 134
\end{array} \right)
\end{equation}
```

Note the argument now has the pipe "|" included to indicate the placement of the vertical rules.

G. Cases Structures

Many times cases can be miscoded using the wrong environment, i.e., `array`. Using the `cases` environment will save keystrokes (from not having to type the `\left\lbrace`) and automatically provide the correct column alignment.

$$z_m(t) = \begin{cases} 1, & \text{if } \beta_m(t) \\ 0, & \text{otherwise.} \end{cases}$$

is coded as follows:

```
\begin{equation*}
{z_m(t)} =
\begin{cases}
1,&{\text{if}}\ {\beta }_m(t),\\
{0,}&{\text{otherwise.}}
\end{cases}
\end{equation*}
```

Note that the "&" is used to mark the tabular alignment. This is important to get proper column alignment. Do not use `\quad` or other fixed spaces to try and align the columns. Also, note the use of the `\text` macro for text elements such as "if" and "otherwise."

H. Function Formatting in Equations

Often, there is an easy way to properly format most common functions. Use of the `\` in front of the function name will in most cases, provide the correct formatting. When this does not work, the following example provides a solution using the `\text` macro:

$$d_R^{KM} = \arg\min_{d_l^{KM}} \{d_1^{KM}, \ldots, d_6^{KM}\}.$$

is coded as follows:

```
\begin{equation*}
 d_{R}^{KM} = \underset {d_{l}^{KM}}
 {\text{arg min}} \{ d_{1}^{KM},
 \ldots,d_{6}^{KM}\}.
\end{equation*}
```

I. Text Acronyms Inside Equations

This example shows where the acronym "MSE" is coded using `\text{}` to match how it appears in the text.

$$\text{MSE} = \frac{1}{n}\sum_{i=1}^{n}(Y_i - \hat{Y}_i)^2$$

```
\begin{equation*}
 \text{MSE} = \frac {1}{n}\sum _{i=1}^{n}
(Y_{i} - \hat {Y_{i}})^{2}
\end{equation*}
```

XIII. Conclusion

The conclusion goes here.

ACKNOWLEDGMENTS

This should be a simple paragraph before the References to thank those individuals and institutions who have supported your work on this article.

APPENDIX
PROOF OF THE ZONKLAR EQUATIONS

Use `\appendix` if you have a single appendix: Do not use `\section` anymore after `\appendix`, only `\section*`. If you have multiple appendixes use `\appendices` then use `\section` to start each appendix. You must declare a `\section` before using any `\subsection` or using `\label` (`\appendices` by itself starts a section numbered zero.)

REFERENCES SECTION

You can use a bibliography generated by BibTeX as a .bbl file. BibTeX documentation can be easily obtained at: http://mirror.ctan.org/biblio/bibtex/contrib/doc/ The IEEEtran BibTeX style support page is: http://www.michaelshell.org/tex/ieeetran/bibtex/

SIMPLE REFERENCES

You can manually copy in the resultant .bbl file and set second argument of `\begin` to the number of references (used to reserve space for the reference number labels box).

REFERENCES

[1] The Radicati Group, "Email statistics report 2019-2023 executive summary," Technical report, The Radicati Group, 2019.
[2] Rick Wash. How experts detect phishing scam emails. Proceedings of the ACM: Human Computer Interaction, CSCW(160), October 2020.
[3] MacEwan University. University Discovers Online Fraud. Press Release, 2017. https://www.macewan.ca/wcm/MacEwanNews/PHISHING_ATTACK.
[4] Rebecca Smith. How a U.S. Utility Got Hacked. Wall Street Journal, Dec 2016.
[5] Eric Lipton, David E Sanger, and Scott Shane. The Perfect Weapon: How Russian Cyberpower Invaded the U.S. The New York Times, dec 2016.
[6] Verizon. 2019 Data Breach Investigations Report. Technical report, 2019.
[7] Symantec. Internet Security Threat Report. Technical Report February, 2019.
[8] Jason Hong. The state of phishing attacks. Communications of the ACM, 55(1):74, Jan 2012.
[9] Joshua T Goodman, Paul S Rehfuss, Robert L Rounthwaite, Manav Mishra, Geoffrey J Hulten, Kenneth G Richards, Aaron H Averbuch, Anthony P Penta, and Roderict C Deyo. Phishing detection, prevention, and notification, October 16 2012. US Patent 8,291,065.
[10] *Mathematics Into Type*. American Mathematical Society. [Online]. Available: https://www.ams.org/arc/styleguide/mit-2.pdf
[11] T. W. Chaundy, P. R. Barrett and C. Batey, *The Printing of Mathematics*. London, U.K., Oxford Univ. Press, 1954.
[12] F. Mittelbach and M. Goossens, *The LaTeXCompanion*, 2nd ed. Boston, MA, USA: Pearson, 2004.
[13] G. Grätzer, *More Math Into LaTeX*, New York, NY, USA: Springer, 2007.
[14] M. Letourneau and J. W. Sharp, *AMS-StyleGuide-online.pdf,* American Mathematical Society, Providence, RI, USA, [Online]. Available: http://www.ams.org/arc/styleguide/index.html
[15] H. Sira-Ramirez, "On the sliding mode control of nonlinear systems," *Syst. Control Lett.*, vol. 19, pp. 303–312, 1992.
[16] A. Levant, "Exact differentiation of signals with unbounded higher derivatives," in *Proc. 45th IEEE Conf. Decis. Control*, San Diego, CA, USA, 2006, pp. 5585–5590. DOI: 10.1109/CDC.2006.377165.
[17] M. Fliess, C. Join, and H. Sira-Ramirez, "Non-linear estimation is easy," *Int. J. Model., Ident. Control*, vol. 4, no. 1, pp. 12–27, 2008.
[18] R. Ortega, A. Astolfi, G. Bastin, and H. Rodriguez, "Stabilization of food-chain systems using a port-controlled Hamiltonian description," in *Proc. Amer. Control Conf.*, Chicago, IL, USA, 2000, pp. 2245–2249.

BIOGRAPHY SECTION

If you have an EPS/PDF photo (graphicx package needed), extra braces are needed around the contents of the optional argument to biography to prevent the LaTeX parser from getting confused when it sees the complicated `\includegraphics` command within an optional argument. (You can create your own custom macro containing the `\includegraphics` command to make things simpler here.)

If you include a photo:

Michael Shell Use `\begin{IEEEbiography}` and then for the 1st argument use `\includegraphics` to declare and link the author photo. Use the author name as the 3rd argument followed by the biography text.

If you will not include a photo:

John Doe Use `\begin{IEEEbiographynophoto}` and the author name as the argument followed by the biography text.