Que tan segura é unha contrasinal?

Daniel López Mendoza

Jacobo Torres Villar

Curso escolar: 2025/2026

3º curso da ESO (Educación Secundaria Obrigatoria)

Contido

Introdución

Hoxe en día, é importante ter coidado cos correos electrónicos enganosos, xa que poderías ser vítima dunha estafa custosa. Este tipo de ciberataques coñécense como phishing. Un ciberdelincuente envíache unha mensaxe ou correo electrónico solicitando información persoal, a miúdo usando frases ou detalles deseñados para que actúes rapidamente e non penses dúas veces sobre se é lexítima. Se proporcionas a información solicitada, o ciberdelincuente pode usala para calquera propósito, poñendo en perigo os teus datos persoais e as túas contas dixitais, como as contas bancarias ou de entretemento (INCIBE, 2026).

Máis do 90 % dos ciberataques comezan con correos electrónicos enganosos. En 2025, os ataques de phishing aumentaron un 1265 % a nivel mundial, impulsados pola IA xerativa. O phishing e as súas variantes (vishing , smishing) representan o 30 % dos incidentes nas organizacións (UAO, 2026).

Agora tes que ter moito coidado co correo electrónico e non premer en nada sen ler a mensaxe dúas veces. Os informes indican que o 20 % das mensaxes de phishing conseguen o seu obxectivo, incluído o de atrapar a profesionais cualificados. Máis do 80 % dos empregados poden "morder o anzol" en simulacións de phishing. Pero en 90 días, se se implementa formación, esa porcentaxe pódese reducir nun 40 % en 3 meses (Garzón Yánez, 2024).

Sería incorrecto pensar que a xente máis nova, por ter nacido nunha época con tanta tecnoloxía, é inmune a estas estafas, xa que estudos recentes indican que a Xeración Z e os Millennials tenden a caer máis nestas trampas (39%-43%) debido á súa confianza nas súas habilidades dixitais, en comparación cos grupos de idade máis maiores (INCIBE, 2026).

Cada día envíanse 3.400 millóns de correos electrónicos de phishing en todo o mundo, o que pón en risco a millóns de persoas (INCIBE, 2026).

Mesmo con todo este perigo, existen técnicas ou trucos para identificar se un correo electrónico é phishing ou seguro:

O primeiro truco é comprobar algunhas cousas: o enderezo de correo electrónico, o contido, o asunto, o título e o nome do ficheiro ou a ligazón. Se algún destes datos che parece sospeitoso ou contén erros ortográficos, o máis probable é que sexa unha estafa.

O seguinte paso sería buscar sinais de IA, xa que revolucionou o phishing. Este tipo de mensaxes adoitan empregar a intelixencia artificial para apoiar as súas afirmacións e facer que as creas. Por exemplo, podes recibir unha mensaxe cun vídeo do teu pai pedíndoche o DNI para que poidas apuntarte a un campamento de verán, e el pídeo urxentemente porque é unha oferta por tempo limitado. Neste caso, necesitamos comprobar se hai anomalías nos detalles, como obxectos no fondo que non obedecen as leis da física ou formas borrosas. Tamén podemos buscar se a textura da persoa é demasiado perfecta, lisa ou brillante, xa que isto tamén podería indicar a IA. Outra pista sería se os movementos dos beizos non coinciden co audio.

Pero imaxinemos que caíches na trampa; ter un contrasinal forte pode reducir os danos. Un contrasinal forte dificulta que un atacante o reutilice noutras contas, limita o acceso se usas contrasinais diferentes para cada servizo e, o máis importante, reduce os ataques automatizados de probas masivas. Os ataques automatizados de probas masivas son ciberataques dirixidos a grande escala que usan bots , scripts e ferramentas automatizadas para

probar miles ou millóns de combinacións, vulnerabilidades ou credenciais nun tempo moi curto. Por iso é tan importante ter un contrasinal forte, pero ***que fai que sexa un contrasinal forte*** ?

Pregunta de investigación

Ata que punto a variedade de caracteres, as letras maiúsculas/minúsculas e a lonxitude do contrasinal afectan o nivel de seguranza do contrasinal creado?

Hipótese

Aumentar a variedade de letras maiúsculas/minúsculas, símbolos, números e lonxitude de caracteres aumenta a seguridade do teu contrasinal porque os piratas informáticos tardarán máis en descifralo, o que os levará deixar de intentalo e probar outros contrasinais máis sinxelos.

Variables

- **Independentes** : lonxitude, variedade de caracteres, variedade de maiúsculas e minúsculas.
- **Dependentes** : Seguridade por contrasinal
- **Control** : a combinación de varias variables independentes ao mesmo tempo.

Materiais

- Un ordenador
- Motor de busca: Google
- Ligazón ao sitio web : Que tan segura é a miña contrasinal? - https://www.security.org/how-secure-is-my-password/
- Programa informático: *Microsoft Excel*

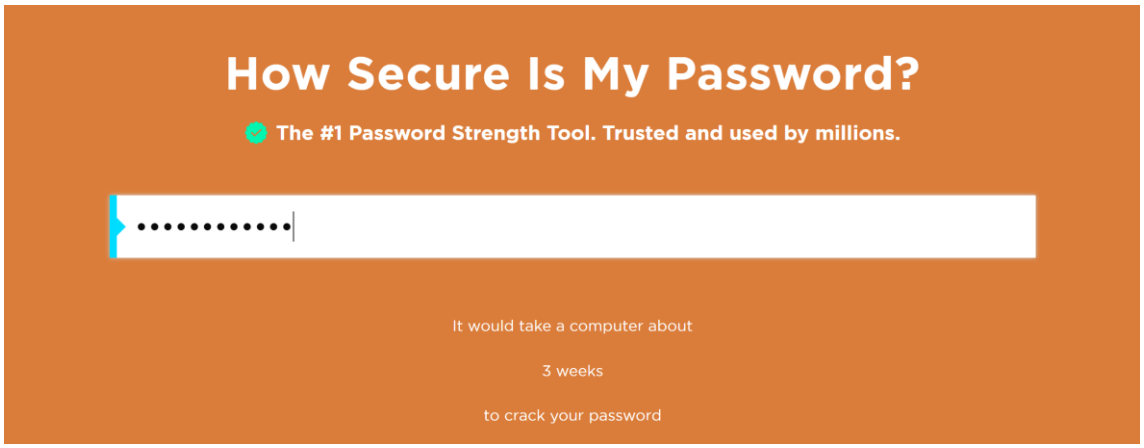
Proceso experimental

O primeiro paso é abrir a páxina web que nos guiará polo proceso: https://www.security.org/how-secure-is-my-password/

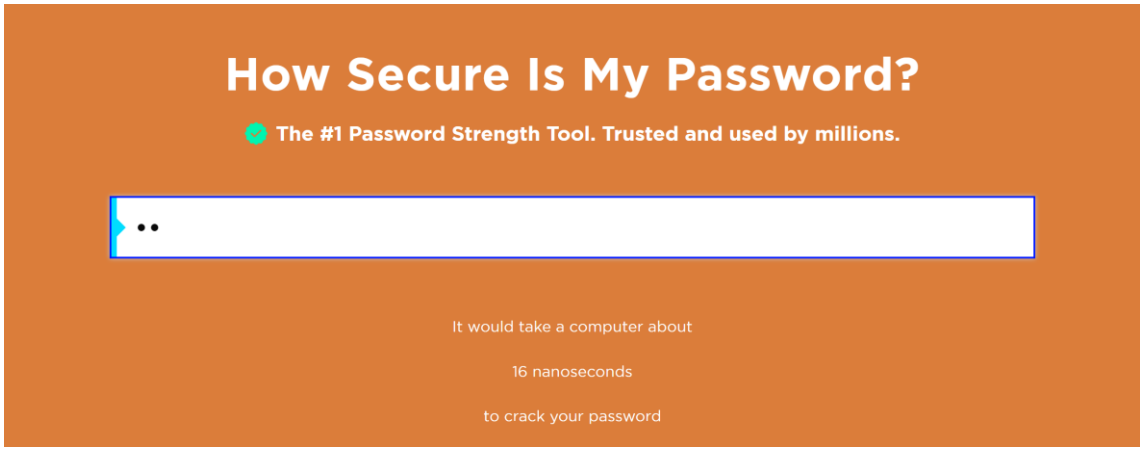
folla de cálculo *de Microsoft Excel* onde crearemos unha serie de contrasinais para avaliar as variables. Un exemplo sería: (AA, Aa , aa ; +++, ++a, ++6, aaa , aa +, aa6, 666, 66a, 66+, a6+; aaa , aaaaaa , aaaaaaaaa , aaaaaaaaaaa ,). Creamos tres táboas nesta folla de cálculo para cada variable independente; a primeira columna conterá o contrasinal e a segunda, o tempo que tarda en descifralo.

Probamos cada contrasinal e rexistramos o resultado de canto tempo tardaría un pirata informático en descifrala en Excel.

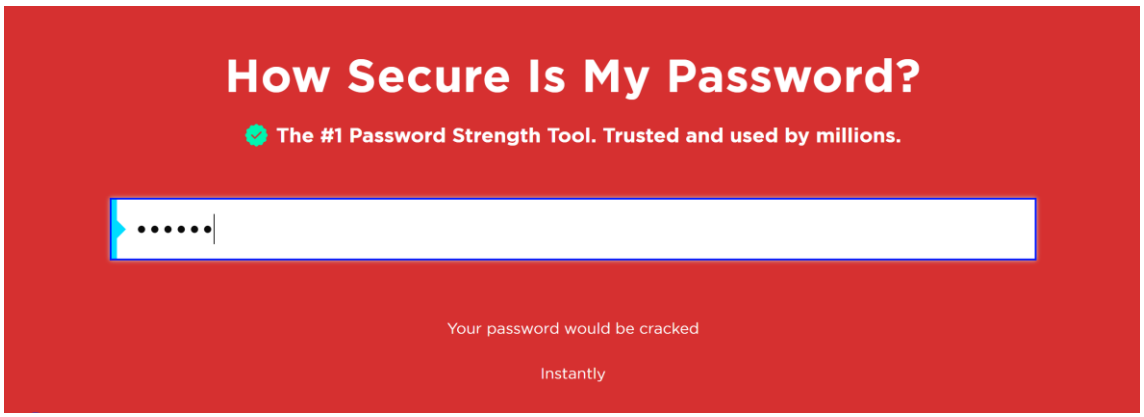
Con todos os resultados á man, destacamos o mellor en función do marco temporal para cada variable. Despois realizamos unha análise (imaxes 1 a 3).



A imaxe 1mostra un exemplo de como introducimos un contrasinal e levounos relativamente máis tempo en comparación cos demais.



A imaxe 2mostra un exemplo de como introducimos un contrasinal e deunos un tempo extremadamente curto en comparación cos outros.



A imaxe 3mostra un exemplo dun contrasinal que se descifraría instantaneamente.

Análise de resultados

A táboa 1 mostra o tempo que leva descubrir o contrasinal en función do número de letras maiúsculas/minúsculas empregadas na súa creación, así como da variedade de caracteres empregados e da lonxitude do contrasinal.

Táboa 1Equivalencia entre o tipo de contrasinal e o tempo que tarda en atopalo. 1 minuto = 0,0167 horas (≥0,000694 días / ≥ 0,00000198) – 1 minuto = 60 segundos (≥ 60.000 milisegundos / ≥ 60.000.000 microsegundos / ≥ 60.000.000.000 nanosegundos).

Contrasinal Maiúsculas e minúsculas	Tempo
AA	16 ns
Aa	67 ns
aa	16 ns
Variedade de personaxes	
+++	900 ns
++6	300 ms
++a	1 ms
aaa	400 ns
aa6	1 ms
aa +	1 ms
666	24 ns
66+	300 ns
66a	1 ms
a6+	3 ms
Lonxitude	
aaa	400 ns
aaaaaa	0
aaaaaaaa	2 minutos
aaaaaaaaaaa	3 semanas
aaaaaaaaaaaa	1000 e

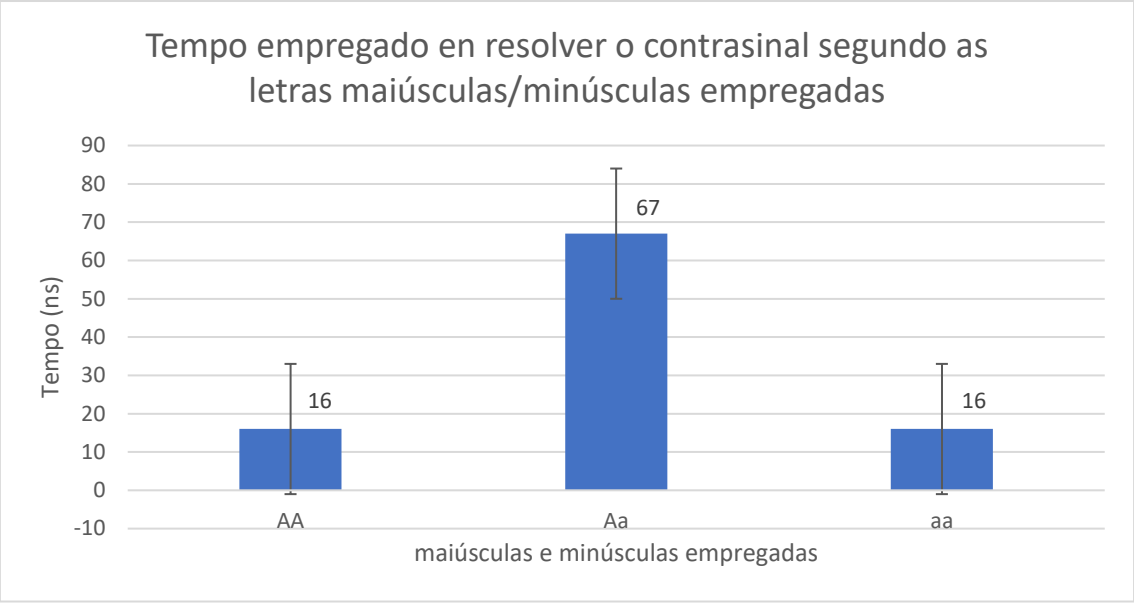


Figura 4Gráfico que mostra o tempo que tarda en recoñecerse un contrasinal en función das letras maiúsculas/minúsculas presentes no contrasinal. (Traballo propio do autor.)

Na imaxe 4, podemos ver que a variación de maiúsculas e minúsculas afecta o tempo que tarda un pirata informático en descifrar un contrasinal. Sen variación de maiúsculas e minúsculas, como podemos observar, só tarda 16 nanosegundos, mentres que coa variación de maiúsculas e minúsculas, tarda ata 67 nanosegundos. Polo tanto, estes resultados demostran que unha combinación de maiúsculas e minúsculas aumenta significativamente o tempo que tarda en descifrar un contrasinal.

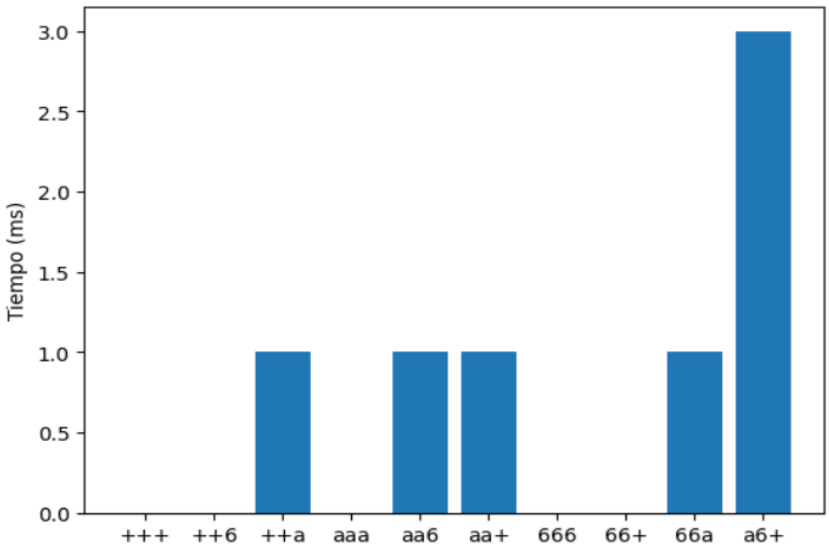


Figura 5Gráfico que mostra o tempo que tarda en recoñecer un contrasinal en función da variedade de letras, números e símbolos presentes nel. (Traballo propio do autor.)

Na imaxe 5, podemos ver como a variedade de caracteres (letras, símbolos e números) afecta o tempo que leva descodificar un contrasinal. Como podemos ver, canta máis variedade, máis segura é a contrasinal. Os contrasinais como ++a só tardan aproximadamente un microsegundo en descodificarse, mentres que o contrasinal a6+ tarda 3 microsegundos, superando a todos os demais. Isto confirma que a variedade ten un efecto positivo.

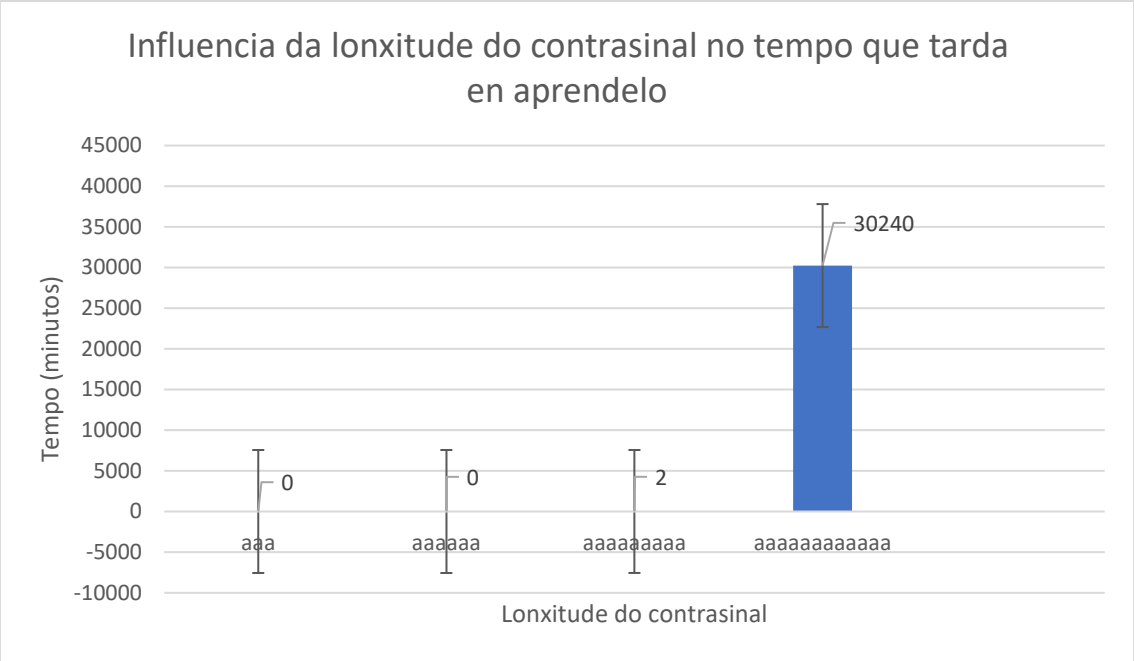


Figura 6Gráfico que mostra o tempo que tarda en recoñecer un contrasinal en función da súa lonxitude. (Traballo propio do autor.)

A imaxe 6 mostra o tempo que tardaría un pirata informático en descifrar un contrasinal en función da súa lonxitude . Sen dúbida, canto máis longo sexa o contrasinal, máis seguro será, xa que, como podemos ver, o contrasinal máis longo ocupa a posición máis alta, mentres que os outros son apenas visibles debido á escala necesaria para o máis longo.

Conclusión

Como amosan os resultados experimentais, a lonxitude do contrasinal, a diversidade de maiúsculas e minúsculas e a variedade de caracteres afectan á seguridade do contrasinal. Polo tanto, a miña hipótese está validada.

Dificultades e melloras na miña metodoloxía

Como mellora, suxeriría poder analizar a seguridade dos patróns de contrasinais en teclados, como qwerty ou qazwsxedc . Tiven dificultades para atopar un sitio web seguro e recomendado para comprobar os contrasinais, xa que moitos deles non son seguros.

Bibliografía

Que é o phishing? - Definición, exemplos de ataques e moito máis | Proofpoint ES . (30 de setembro de 2025). Proofpoint . https://www.proofpoint.com/es/threat-reference/phishing

Experto, GPHS (13 de outubro de 2025). *Que tan segura é a miña contrasinal? | Verificador de forza de contrasinal* . Security.org. https://www.security.org/how-secure-is-my-password/

Protéxase da suplantación de identidade (phishing): soporte técnico de Microsoft (sf). https://support.microsoft.com/en-us/windows/protect-yourself-from-phishing-0c7ea947-ba98-3bd9-7184-430e1f860a44#:~:text=Phishing%20is%20a%20popular%20form,respond%20with%20their%20personal%20information .

Araujo, A. e Araujo, A. (15 de xaneiro de 2026). *Introdución á suplantación de identidade (phishing): que é, como funciona e tipos* . Blog de Hackmetrix . https://blog.hackmetrix.com/que-es-el-phishing/#:~:text=%E2%80%9CWhishing%E2%80%9D%2C%20%E2%80%9CWhatsapping%E2%80%9D,amigos%20para%20obter%20información%C3%B3n%20personal .

Magazine, P. (25 de abril de 2025). *As 10 marcas máis suplantadas en phishing en 2025: Microsoft, Google e Apple lideran a clasificación* . PYMES MAGAZINE. https://pymesmagazine.es/actualidad/las-10-marcas-mas-suplantadas-por-phishing-en-2025-microsoft-google-y-apple-lideran-el-ranking/#:~:text=El%20%C3%BAltimo%20Brand%20Phishing%20Report%20publicado%20por,de%20Microsoft%20para%20enga%C3%B1ar%20a%20los%20usuarios .

Baker, E. (sf). *Informe de tendencias de phishing (actualizado para 2025)* . https://hoxhunt.com/guide/phishing-trends-report#:~:text=QR%20code%20phishing%20attacks%20(quishing,business%20cards%20to%20lure%20victims.&text=A IA está a impulsar os ataques de suplantación de identidade, persoas en finanzas e recursos humanos.&text=Os atacantes están a explotar cada vez máis as plataformas, un cambio nestes canais.&text=Os correos electrónicos de suplantación de identidade imitan os organismos gobernamentais, sobre impostos atrasados ou multas.&text=A dispoñibilidade de Listo para, esquemas de phishing de alta calidade, E2%80%8B.&text=Os atacantes%20frecuentemente%20suplantan%20a%coñecidos, UpGuard%20e%20Trend%20Micro%20News .

Que é a suplantación de identidade (phishing)? | Seguridade de Microsoft . (s.d.) . https://www.microsoft.com/es-es/security/business/security-101/what-is-phishing#:~:text=The%20consequences%20of%20phishing%20can%20be%20ser%20graves,your%20information%20has%20put%20in%20danger

Data, I. (20 de novembro de 2023). *Que é o phishing e como protexerse* . IPDATA. https://ipdata.es/que-es-el-phishing-conoce-la-amenaza-y-protegete/

https://chequeado.com/ultimas-noticias/como-saber-si-una-imagen-fue-creada-con-inteligencia-artificial/#:~:text=Si%20no%20coñecemos%20o%20origen%2C%20podemos%20facer,con%20Google%20u%20outro%20buscador%20como%20Tineye .

García, P. (18 de febreiro de 2026). Ciberataques en España en 2025: cifras do INCIBE e puntos clave para 2026. *PentestingTeam* . https://pentestingteam.com/blog/ciberataques-espana-2025-incibe-claves/#:~:text=En%20Februario%20de%202026%20o%20Instituto%20Nacional,presenza%20de%20malware%2C%20ransomware%2C%20fraudes%20e%20phishing%2C

Cibersecurity.io . (12 de febreiro de 2026). *Os ciberataques en España aumentarán un 26 % en 2025: o malware e o phishing lideran un ano récord* . Cibersecurity.io. https://www.cibersecurity.io/los-ciberataques-en-espana-se-disparan-un-26-en-2025-malware-y-phishing-lideran-un-ano-record/#:~:text=Los%20ciberataques%20en%20Espa%C3%B1a%20se,un%20a%C3%B1o%20r%C3%A9cord%20%2D%20Cibersecurity.io

Xestión segura de contrasinais | Cidadanía | INCIBE . (n.d.). https://www.incibe.es/ciudadania/tematicas/contrasenas-seguras

CrowdSec . (19 de decembro de 2024). *Que son os ataques de explotación masiva? | CrowdSec* . https://www.crowdsec.net/glossary/mass-exploitation-attacks

11 consellos para detectar correos electrónicos maliciosos . (10 de abril de 2023). Globalsign . Recuperado o 19 de febreiro de 2026 de https://www.globalsign.com/es/blog/11-tips-for-detecting-malicious-emails