G Data press release 2014

sid 14: Pentru un Internet mai bun

G Data ii invita pe utilizatorii de Internet la Safer Internet Day 2014

Bucuresti (Romania) 06.02.2014

Chiar daca ne referim la tineri sau varstnici, una din trei persoane de pe glob sunt online (sursa: BITKOM). Cu toate acestea, multi dintre acesti utilizatori sunt departe de a fi constienti de riscurile si pericolele de pe World Wide Web, iar aceasta abordare ii duce direct in bratele infractorilor. Sub sloganul "Let's create a better Internet together", cea de-a zecea zi Safer Internet de martea viitoare isi propune sa aduca o mai mare vizibilitate asupra pericolelor de pe Internet. G Data sprijina actiunea la nivel global si indeamna utilizatorii sa acorde mai multa atentie. Providerul german de securitate IT ii ajuta pe utilizatori sa faca acest lucru oferindu-le acestora cateva sfaturi usor de aplicat.

De ani buni, G Data a observat o crestere a numarului de programe malware si atacuri asupra utilizatorilor de computere si dispozitive cu Android. Dar, chiar si acum, multi utilizatori de Internet nu sunt constienti asupra riscurilor si pericolelor asociate cu navigarea pe Internet. *"Utilizatorii de Internet au nevoie sa stie foarte clar despre pericolele de pe Internet. Doar stiind ce trucuri si inselatorii folosesc infractorii, se vor putea proteja singuri,"* explica Eddy Willems, G Data Security Evangelist.

Atacatorii ii vizeaza pe utilizatorii neavizati, in special pentru a le subtiliza datele personale, de genul parolelor pentru magazine online, conturi bancare sau casute de email. *"Infractorii tintesc informatii pe care le pot folosi pentru a face bani pe piata neagra," spune expertul.* Eddy Willems nu ii consiliaza doar pe adulti – copiii sunt, de asemenea, o tinta profitabila. De aceea, expertul in securitate sfatuieste: *"Parintii ar trebui sa nu se gandeasca doar la propria securitate, ci si la securitatea copiilor lor. In afara utilizarii unei solutii de securitate si instalarea actualizarilor de program disponibile, ei ar trebui sa fie vigilenti cand utilizeaza Internetul."*

Sfaturi de securitate de la G Data, pentru tineri si varstnici, la sid 14

- Protejati de programe de securitate: O solutie puternica de securitate este o parte din echipamentul de baza al oricarui computer conectat la web. Acesta trebuie sa includa, pe langa protectia antivirus, si un filtru antispam, firewall si protectie in timp real impotriva amenintarilor online.
- Inchideti bresele de securitate: Trebuie sa folositi actualizarile pentru a va asigura ca sistemul de operare, programele si aplicatiile utilizate sunt actualizate

permanent. Aceasta ii va ajuta pe utilizatori sa inchida bresele ce pot fi exploatate de infractori.

- Trimiteti direct in cosul de gunoi digital: Stergeti imediat spamul primit pe email si evitati accesarea link-urilor incluse sau a fisierelor atasate.
- Parole sigure: Pentru orice cont online, de exemplu retele sociale si provideri de servicii de email, trebuie sa folositi parole diferite ce constau in combinatii lipsite de logica ce includ numere, litere mici si majuscule.
- Backup de date: Utilizatorii ar trebui sa-si salveze datele importante, astfel incat sa poata fi restaurate dupa o eventuala distrugere a sistemului sau in urma unei infectari. Solutiile comprehensive de securitate includ de regula si un modul de backup.
- Copii in siguranta pe Internet: Parintii trebuie sa-si invete copiii cum sa utilizeze Internetul in siguranta. Modulul de control parental usureaza sarcina parintilor si previne accesarea site-urilor cu continut inadecvat, de genul droguri, violenta sau sex.

Smartphone-uri si tablete

- Instalati o solutie de securitate: O aplicatie de securitate este esentiala pentru dispozitivele cu Android. Aplicatia trebuie sa ofere o protectie adecvata impotriva aplicatiilor malware.
- Aplicatii de incredere: Aplicatiile ar trebui descarcate doar din surse de incredere, precum Google Play for Android. Cand selectati o aplicatie, trebuie sa acordati atentie autorizarilor pe care le cere.
- Activati functiile Bluetooth si GPS doar la nevoie: Utilizatorii ar trebui sa dezactiveze serviciile wireless, precum WLAN, GPS si Bluetooth dupa utilizare.
- Verificati setarile de securitate: Utilizatorii ar trebui sa activeze functia de introducere a parolei si sa inlocuiasca parola standard cu una personala.

Retele sociale

- Nu toti iti sunt prieteni: Este recomandat sa acceptati cererile de prietenie doar daca stiti dinainte cine este in spatele acestora.
- Atentie la URL-uri scurte: Link-urile abreviate pot conduce catre o capcana malware. Utilizatorii ar trebui sa trateze cu suspiciune si sa nu acceseze URL-urile primite de la necunoscuti.

- Nu dezvaluiti prea multe depre propria persoana: Utilizatorii retelelor sociale ar trebui sa nu ofere prea multe informatii personale si sa nu publice adresa sau numarul de telefon.