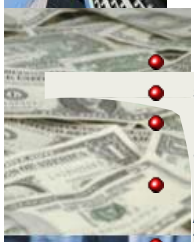
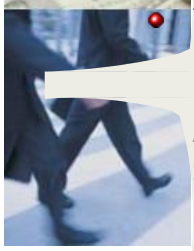
Issue 4 | Volume 8 | Dec. 2021





Security Solutions

ADDRESSING THE NEEDS AND SECURING THE FUTURE

Helping secure your world

Editor's Note

2021 started, continued, and will end in the unrelenting grip of the CoVid-2019 global pandemic. No one was prepared for this, as it has continuously created new trepidations which evolved into new approaches in security and how we as individuals deal with this seemingly never-ending pandemic.

With lockdowns being lifted in some regions, other countries are continuing with this method to stem the fourth and fifth waves, meaning persons are still required to do everything from home.

The first article speaks about simple cyber security rules to follow at home. The second article asks a relevant question and teaches persons how to identify cracked software because knock-offs and cheaper software isn't always better.

In keeping with the theme of safety, the next article examines how one can improve insurance website security. One easy way to do this is by restricting access and user roles because each assigned user role allows for a set of tasks to be performed which are called capabilities. You can learn more about this by reading article number three.

Article four discusses the top keywords used in phishing email subject lines. This is very important as these scams can set you back thousands of dollars in losses through illegitimate means of accessing your bank account and personal funds.

We do hope you find these articles and the safety methods helpful in some manner. We at Amalgamated Security Services Limited will hold steadfast and continue to fulfill our commitment, which is to provide quality service for all customers.

Regards
Carril Reyes-Telesford
Senior Marketing Officer

5 Simple Cybersecurity Rules To Follow At Home

By George Rosenthal

Much has been written about proper cybersecurity safeguards for those working from remote locations.

While remote workers need to be aware and educated regarding precautions to guard against a data breach to their corporate business network, the same holds true for those using their devices for mostly leisure activities.

Taking some necessary precautions need not be complicated. In fact there are many simple measures anyone can utilize at home to prevent themselves from becoming a victim of a cybercrime. These include...

1. Utilizing longer passwords.

Most individuals utilize short, easy to remember passwords. While seemingly harmless, simple and insecure passwords are one of the most common ways you can leave yourself susceptible to a cyberattack.

Passwords that are easy to remember are also easy to hack.

A basic rule is to use passwords that always contain a mix of uppercase and lowercase letters, as well as numbers. A symbol or two can be added for extra security. Also avoid the temptation to write all your passwords down on paper.

2. Creating different passwords for different accounts.

Many of us are guilty of using the same password on multiple accounts. Utilization of different passwords adds a high degree of difficulty for any cyber thief attempting to penetrate one or more of your accounts.

Passwords should also be changed regularly. This again helps to mitigate the damage if a password is stolen, because the hacker won't have access to all of your other accounts.

3. Avoiding the placement of sensitive information on social media.

Many individuals unknowingly reveal private or sensitive information on their public social channels.

Something as simple as posting a photo that you are on vacation could provide the impetus for someone to break into your home.

Social media accounts should be kept private so only trusted friends and family can view your posts.

Never accept friend requests from people you don't know, and be wary of those with duplicate accounts.

Also be wary of friends direct-messaging with strange links or requests for money. If their behavior seems out of the ordinary, or their manner of communicating seems different, a hacker could have obtained access to their account.

4. Becoming more deliberate about accepting app privileges.

When a new app is installed on your phone, it often requests access to certain privileges like your location.

This collection of data may be necessary for the app to function, but some apps could be less trustworthy. Take special care with smaller, less common apps.

Before automatically granting privileges, consider if the

request makes sense. If it doesn't, don't grant access. Location-sharing privileges are especially risky, as they can reveal where you are to anyone online.

5. Taking a proactive approach with antivirus software.

Trusted antivirus software should be installed on all devices. Viruses can reach your computer in a variety of ways, and good antivirus software will guard against them. The goal is to keep them from wreaking havoc on your system as they remain undetected.

Software should be kept up-to-date to guard against all the latest digital threats. This includes the avoidance of leaving devices on standby for long periods of time.

Instead computers should be restarted and updated on a regular basis. This enables software providers to upgrade any potential flaw in their system and add the highest level of protection to maintain the optimal cybersecurity available.

Creating a number of cybersecurity precautions will protect you and your family, as well as your coworkers, and your employer. Cyberattacks can come at any time, and all it takes is one unknowing error to be in serious trouble.

Article
Source: https://EzineArticles.com/expert/George_Rosenthal/2014004

Amalgamated Security Services offer a full range of security service solutions which are inclusive of the following:

Response Services
Alarm Monitoring
Guarding Services
Electronic Service
Courier Services
Assess Controls
Data Services
Cash Services
Investigations

Don't Fall for the Money-Saving Lure of Cracked Software

Think you've found a bargain price for that expensive app or software you need? Like most other too-good-to-be-true deals, it's probably a scam. Not only that, but if you use it, you could be breaking the law. We're talking about so-called "cracked" software -- an app that has been cracked open to remove its protection so that anyone can use or copy it, sometimes without paying a cent.

The Internet is teeming with the stuff. There are hundreds, maybe thousands, of websites dedicated to cracks. You might think it's worth a try, but don't even go there.

Here's one reason why: When you buy cracked software, you're often advised to switch off your Internet security app to enable you to install it. This sometimes happens with

genuine software, so it's hard to spot the ruse. If and when you do, you have nothing to protect you from the malware that can be hidden inside the modified software.

Furthermore, you might not even get the app you're trying to get on the cheap or for free. In a malware storm that's raging on the Internet right now, crooks are using an evil tactic where they may not supply even a cracked program; they just install a bit of code called Mosaic Loader, which unlocks access to your PC. While it's being installed, it mimics the real program misguided downloaders are trying to get, even using the same file and folder structure. That means victims won't discover what's happened until it's too late!

Before they know it, every bit of confidential data on a PC could be stolen, or the machine will be locked into a network of computers used for sending out spam or other malware.

In other words, your system will be cracked open too.

Dark Web

Security researchers believe a global team of hackers behind the current onslaught plans to break into as many computers as possible, as fast as possible, and then actually sell access to other crooks and scammers via the black market (the "Dark Web").

In one case, reported by security firm Sophos, an overseas company is reputedly offering $5 for each link to compromised PCs.

In a "refinement" of the scam, the malware actually produces a pop-up warning of infection, with a "help" link that actually leads to even more malware disguised as a removal tool. This is dangerous stuff. What might have started out as an attempt to get something for nothing could prove to be a horrendously expensive mistake.

Here are three ways to avoid getting caught up in this minefield.

First, don't buy dirt-cheap versions of expensive software. It's probably a scam, but even if it works and isn't infected, it won't be supported by the developer, you can't troubleshoot it, and it could damage your operating system. Plus, it may also be illegal, even when the crack site says it's not. You can face fines of up to $250,000 or even get jail time if you pass it to someone else.

Don't even search for cracked software. If you Google the term, you'll see pages and pages of crack sites, often offering links to the Top 10 sources. You have absolutely no way of knowing what they're up to.

Second, be ultra-cautious about switching off your security software before installing any program, especially downloaded or cut-price software. Instead, create a restore point on a Windows PC (here's how: https://support.microsoft.com/en-us/windows/create-a-system-restore-point-77e02e2a-3298-c869-9974-ef5658ea3be9) and try the installation with your security program intact. If it doesn't work, the restore point will enable you to backtrack.

If you really must suspend your security, do it for as little time as possible and then run a scan immediately after the installation.

And third, if the software you want is too expensive, look for an alternative, not a crack. For example, there are half a dozen legitimate and free or low-cost word-processing programs that, for most people, perform just as well as full-cost ones and offer compatibility with their expensive cousins.

According to the Digital Citizens Alliance, one third of illegal and cracked software is infected with viruses, Trojans, adware, and spyware. Those are frightening odds. Just don't put yourself at risk; stick with the real thing.

If you are interested in learning more about our home security systems visit our website at: http://esis.assl.com/alarms-electronic-products/cctv-systems

Improving Insurance Website Security - Restricting Access & User Roles

By Alan Blume

WordPress is the most popular and pervasive website content management platform on the market, with market share estimated by some to be over 60%. Website owners (or those responsible to maintain their Insurance WordPress sites) can and should manage user access to tasks such as writing and editing, page creation. Category creation, comment moderation, plugin and theme management, user management, by assigning specific roles to all users.

WordPress Predefined Roles:

1. Super Admin
2. Administrator
3. Editor
4. Author
5. Contributor
6. Subscriber

Role Definitions

- Super Admin: Allows access to all sitewide administration and features. This role should be severely limited, as it is the most powerful, and allows the user to make major site modifications.
- Administrator: Not as powerful as Super Admin, but still has access to all administration features within a single website.
- Editor: Allows users to publish and manage posts, including other users' posts.
- Author: Allows the user to publish and manage their own posts.
- Contributor: Allows the author to write and manage their own posts but does not allow them to publish the content.
- Subscriber: Read only access, allowing the user to review content and manage their profile.

Leveraging the power of user access helps ensure a more secure WordPress website.

Let's begin by discussing roles and tasks.

Each assigned user role allows for a set of tasks to be performed which are called capabilities. There are many

capabilities, a few examples include publishing posts, moderating comments, and editing users. Default capabilities are preassigned to each role, but other capabilities can be assigned or removed, allowing for custom user role creation. Greater control and refinements of user roles will improve overall website security and limit the user errors that can cause security breaches.

Website owners can also harden their WordPress sites using Permission Modes. For example, permissions can specify who and what can read, write, modify, and access directories and files. This is important as WordPress may need access to write to files in your wp-content directory for the site to function properly.

FTP access is another area to address to improve website security. For example, if you need a third-party contractor to modify your site or customize a plugin, they may require FTP access. But you do not have to grant them full access to the root directory of your website. Limit access to the specific area they are working on, such as the theme's directory. Provide support logs if needed instead of granting FTP access to the logs on your site. And make sure the FTP access and password are time limited, expiring in a week or two (as short a duration as possible).

Following these WordPress best practices will help ensure a more secure insurance agency website, employing greater user role restrictions, and limiting website access.

For more information on insurance agency exclusive marketing and lead gen solutions visit our website at https://www.startupselling.com. StartUpSelling, Inc. provides outsourced insurance agency lead generation services focusing in the areas of telemarketing, insurance agency email marketing, and insurance web marketing.

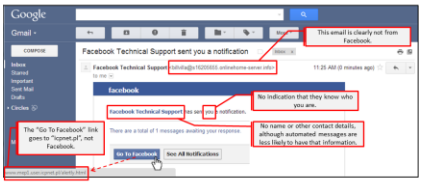
Article
Source: https://EzineArticles.com/expert/Alan_Blume/585514

Amalgamated Security Services offer a full range of security service solutions which are inclusive of the following:

Response Services
Alarm Monitoring
Guarding Services
Electronic Service
Courier Services
Assess Controls
Data Services
Cash Services
Investigations

The top keywords used in phishing email subject lines

by **R. Dallon Adams** in **Security**
Some of these phrasings are standard day-to-day subject lines, but as one expert explained, "the attacker wants you to be moving too fast to stop and question if it's legitimate."



In recent months, hacking groups have brought critical aspects of U.S. infrastructure to a halt, and phishing is a popular tool in cybercriminal's seemingly ever-expanding armamentarium of attack methods. On Wednesday, Expel released a report, highlighting the top keywords used in phishing attempt subject lines. Based on the findings, employees may need to be particularly wary of the seemingly innocuous emails in their inboxes.

"Attackers are trying to trick people into giving them their

credentials. The best way to do this is to make the email look legitimate, prompt one clear action and lace it with emotion - urgency or fear of loss are the most common," said Ben Brigida, director, SOC Operations, at Expel. "The actions are as simple as 'go to this site' or 'open this file,' but the attacker wants you to be moving too fast to stop and question if it's legitimate."

Malicious emails: Top phishing attempt keywords

To determine this list of keywords, Expel looked at 10,000 malicious emails. In a blog post about the findings, Expel said the keywords in these subject lines target one or multiple themes in an effort to "make recipients interact with the content." These themes include "imitating legitimate business activities, generating a "sense of urgency" and cueing the "recipient to act."

Some of the top listed phishing keywords are designed to imitate legitimate business invoices.

In order, the top three such subject lines include "RE: INVOICE," "Missing Inv ####; From [Legitimate Business Name] and "INV####."

To add context to these phishing attempts disguised as standard invoices, Expel said that "generic business terminology doesn't immediately stand out as suspicious and maximizes relevance to the most potential recipients by blending in with legitimate emails, which presents challenges for security technology."

Per Expel, subject lines highlighting newness are frequently used in phishing attempts with examples including "New Message from ####, "New Scanned Fax Doc-Delivery for ####" and "New FaxTransmission from ####."

Adding context to this roundup of "new" subject lines, Expel said legit communications and alerts regularly use the term "new" to "raise the recipient's interest," adding that "people are drawn to new things in their inbox, wanting to make sure they don't miss something important."

Subject lines highlighting new messages and further actions requirements are also popular phishing methods, according to Expel, with phrasing focused on expiration notices for emails and passwords, verification requirements and others.

"Keywords that promote action or a sense of urgency are favorites among attackers because they prompt people to click without taking as much time to think. "Required" also targets employees' sense of responsibility to urge them to quickly take action," the post said.

Other top phishing attempt subject lines include blank subject lines, file/document sharing language, service and form requests, action requirements and eFax angles.

Spear phishing: Targeting specific employees

On average organizations will face more than 700 social engineering cyberattacks annually and 10% of the targeted attacks are business email compromises (BEC), according to a July Barracuda Networks report; among social engineering attacks analyzed by company researchers, phishing represented 49%.

Interestingly, a person's role at a company may play a role in their risk of being targeted by cybercriminals. For example,

Barracuda Networks determined that IT professionals receive an average of 40 targeted phishing attacks annually and this number jumps to 57 for CEOs.

Brigida said the subject line action is "ideally" a task the email recipient does in their day-to-day job so that the "request feels familiar or routine."

"If a user is in finance, they may fall for an invoice-themed phish. If they are in recruiting, they may fall for a resume-themed phish," Brigida said. "The job of an attacker is to trick the user into doing what they want, evading security detection tools in the process by blending in with typical business activities."

Reprinted from Tech Republic.com

Amalgamated Security Services offer a full range of security service solutions which are inclusive of the following:

Response Services
Alarm Monitoring
Guarding Services
Electronic Service
Courier Services
Assess Controls
Data Services
Cash Services
Investigations