ISSUE
00
MONTH
YEAR

Tips to Keep You Safe from Ever-Growing Cyber Attacks!

Cyber Aware

This Issue

Human Error Leading Cause of Breaches

"Human Error Remains the Top Security Issue"

- SANS Institute

"Human Error is Biggest Cybersecurity Threat, CTOs Say"

- Technology Magazine

Weak Passwords Invite Cyberattacks

By (Client Name)

Last year, the top 10 weakest passwords were pretty much the same as they were in prior years, which offers a tremendous opportunity for cyberscammers.

Scammers are really good at guessing passwords — the weaker the password, the faster they can crack our code.

How Scammers Work

First, they send us multiple fake emails or texts that look to be legitimate — spoofed emails from people we know or companies we do business with — hoping we click on the fraudulent links they embed.

Maybe it's a "receipt" from Amazon that thanks us for our recent $300 order and asks us to click the link provided if we have questions about the order.

Or maybe it's a special university job offer that sounds way too good to be true.

If you "click here to apply," you will unwittingly allow scammers to install a malicious code into your device that allows them to root around, hoping to find login and password details to gain access to your banking or credit card accounts.

Even if they don't discover the passwords they need, it won't take them but a few seconds to crack the weakest ones.

Simple Passwords Put Users at Risk

According to the password-managing company NordPass, the most commonly used passwords of 2023 are embarrassingly simple-minded.

The most popular password was "123456." Scammers can crack that one in less than one second.

"Admin" is the second-most popular password. It and No. 7, "password," also can

Easy Passwords Enable Scams

"More Than 90% of Cyberattacks Made Possible by Human Error"

- Tech Xplore

"Human Error Cited as Leading Cybersecurity Threat in Orgs"

- SC Magazine

be cracked in less than one second.

If you want to see how easy your passwords are to crack, type them into a password detector, such as this one from Bitwarden.

Easy Passwords Enable Costly Scams

The regrettable fact is, in the digital world in which we all now live, cyberscammers are working overtime to come up with ever-more-clever schemes to defraud us.

For example, ransomware attacks grew exponentially the last few years — particularly at universities.

Ransomware is malicious software that scammers use to encrypt a company's or individual's data and block access to it until a hefty sum of money is paid.

Google the words "ransomware attack" and you'll see a sizable list of individuals, big universities and entire cities that have been completely shut down by increasingly sophisticated scammers.

Another big trend: Activists who support various political causes are launching attacks on individuals, businesses and universities who support their opponents.

Utilities and infrastructure that are using outdated systems are especially vulnerable to attacks.

But our elderly face the greatest risk of cyberfraud because they are much more likely to trust people who email, text or call them than younger generations are.

Strong Password Skills Are Imperative

Improving our password skills is an obvious place to start. Pass phrases are recommended. The longer the password the better.

The more random the password is — a mix of letters, numbers and typographical systems makes for strong passwords — the harder it is for automated password crackers to guess your passwords.

Never reuse a password at more than one website.

And consider investing in a secure password manager, such as one of those recommended in this How- To-Geek article.

Here's what a secure password might look like: "StopScammers1178#@!!in2024&&!!"

According to Bitwarden, it would take scammers centuries to crack that one!