SHARDSECURE

DATA SECURITY FOR NON-IT STAFF

In today's digital landscape, threats to data security are everywhere. From phishing to ransomware, from DDos to XSS to plain old human error, there's a myriad of ways for attackers to gain access to your organization's files.

Luckily, you don't have to be a security expert to keep yourself and your company safe. Our infographic will help you understand the top eight risk areas and take steps to protect yourself.

1. Phishing

Phishing attacks are a form of social engineering where an attacker pretends to be a business or trusted colleague. To stay safe, never offer sensitive information, including passwords and financial information, in response to an unsolicited request by phone, email, or text.

2. Compromised or weak credentials

When usernames and passwords are easily guessed, data is put at risk of leaks, phishing scams, malware attacks, and more. Make sure to create secure passwords and comply with 2FA and MFA security measures.

3. Brute force attacks

Brute force attackers will use a large volume of attempts to guess login credentials until they gain access. Your IT team is your best defense against this kind of threat, but you'll want to use strong passwords so your account isn't the weak link.

4. Misconfigured security settings

When cloud services are misconfigured, unauthorized users may access company data and cause costly breaches and leaks. Your IT team will need to be vigilant about monitoring your business's cloud permissions, and you'll want to speak up if you notice that someone has access to storage locations they shouldn't.

5. Ransomware

Ransomware attackers encrypt data and threaten to either withhold the decryption key or, in a double extortion attack, publish the data unless they receive a sizable ransom payment. To fight ransomware, back up your critical data, don't click on any links or attachments you don't recognize, and educate yourself with some of these resources.

6. Insider threats

Not only disgruntled employees but also careless ones can expose private information, customer data, and company-specific vulnerabilities. Be careful of who you divulge information to, never share login credentials, and double check the recipients of any message containing sensitive data.

7. Third-party vendors

Vendors can pose a significant risk to an organization's data, as in the case of the 2020 SolarWinds attack in which over a hundred companies and government agencies were compromised. If you're the point of contact for a vendor, make sure you don't divulge any sensitive information or grant any unnecessary access.

8. Human error

Even though we know to be careful, accidents happen. Read up on the scale of human error — it might surprise you — and make sure to immediately report any security errors to your team.

We've only scratched the surface of the threat landscape, but with caution and the right tools, you can stay well protected.
ShardSecure's holistic data control platform protects against ransomware, misconfigurations, outages, human error, and more. To learn more about how we're meeting common cyberthreats with strong data security and resilience, check out our resources page today.